CHAPTER 1

製品概要

この章では、Cisco Anomaly Guard Module（Guard モジュール）の概要について説明します。概要には、Guard 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から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。

- Guard モジュールについて
- DDos 攻撃について
- 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
- ゾーン保護について
- 保護サイクルについて
- 1 Gbps と 3 Gbps の帯域幅オプションについて

Guard モジュールについて

Guard モジュールは、DDoS 攻撃（分散型サービス拒絶攻撃）を軽減するデバイスです。Guard モジュールは、疑わしいトラフィックをクリーニングのために通常のネットワーク パスから自分宛に宛先変更します。トラフィック クリーニング プロセス中に、Guard モジュールは、攻撃パケットを識別してドロップし、正当なパケットを目的の宛先ネットワークに転送します。

通常 Guard モジュールは、分散型のアップストリーム構成にバックボーン レベルで導入します。Guard モジュールは、次のシスコ製品のどちらかに設置できます。

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

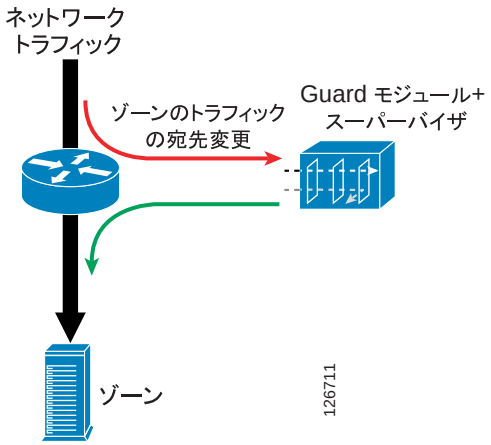
Guard モジュールが DDoS 攻撃から保護するネットワーク要素（つまりゾーン）を定義します。ゾーンが攻撃を受けている場合、Guard モジュールはそのターゲット ゾーン宛のネットワーク トラフィックだけを宛先変更し、特定の攻撃パケットを識別してドロップし、正当なトラフィック パケットをゾーンに転送します。Guard モジュールは常にゾーン トラフィックをフィルタリングし、新たに発生する攻撃に対する警戒を続けます。Guard モジュールは、ゾーンに対する攻撃が終了したと判断すると、ゾーン トラフィックを自分宛に宛先変更することを停止します。Guard モジュールは、必要なときだけネットワーク トラフィックを宛先変更することにより、攻撃時には保護の役割を果たし、それ以外のときにはネットワーク バックグラウンドに控えた状態を保つことができます。

Guard 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。Guard 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 Guard モジュールが使用する参照ポイントを定義します。
- トラフィック保護：正当なトラフィックと悪意のあるトラフィックを区別し、悪意のあるトラフィックをフィルタリングして、正当なトラフィックだけがゾーンに渡されるようにします。
- トラフィックの宛先変更：ゾーン トラフィックを通常のネットワーク パスから Guard モジュールのラーニング プロセスおよび保護プロセスに宛先変更し、正常なゾーン トラフィックをネットワークに戻します。

図 1-1 に、ネットワークでの適用例を示します。ここで、Guard モジュールは、ゾーン トラフィックをラーニングしたり、ゾーンを攻撃から保護したりできるように、ゾーン トラフィックを自分宛に宛先変更しています。

図 1-1　Cisco Anomaly Guard Module 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、何者か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
- 非スプーフィング攻撃について

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。

スプーフィング攻撃を撃退するために、Guard モジュールはスプーフィング防止プロセスを実行します。このプロセスでは、スプーフィングされたトラフィックとスプーフィングされていないトラフィックを区別できるチャレンジ / レスポンス アルゴリズムを使用します。Guard は、スプーフィング防止メカニズムを通過したトラフィックを認証済みトラフィックと見なします。

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。

Guard モジュールは、まず、スプーフィング防止メカニズムをアクティブにして、スプーフィングされたパケットをすべてブロックします。その後、Guard モジュールはトラフィックの統計分析を行い、異常な数の SYN パケット、多数の同時接続、高いトラフィック レートなど、スプーフィングされていないトラフィックの異常を検出してブロックします。

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。Guard モジュールのゾンビ防止プロセスは、チャレンジ / レスポンス認証プロセスを使用して、正当なブラウザと、攻撃対象サイトにアクセスするゾンビ プログラムを区別することで、そのような HTTP 攻撃を軽減します。

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、Guard 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 Guard 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
- ゾーン ポリシーについて
- ラーニング プロセスについて

ゾーンについて

Guard モジュールが保護するゾーンは、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 Guard モジュールによりゾーンに設定されます。

Guard 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 6 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

Guard モジュールは、ゾーンを保護する場合、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し、ゾーンに対する攻撃を軽減できます。トラフィック フローがポリシーしきい値を超えると、Guard 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 セットを動的に設定し、攻撃の重大度に応じて適切な保護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 8 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

Guard 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、分析したトラフィックに基づいて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。Guard モジュールは、ゾーン固有のポリシーおよびポリシーしきい値を使用して、ゾーン トラフィックの異常をより正確に検出できます。

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、Guard 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、Guard 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、Guard 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 9 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。

ゾーン保護について

次のいずれかの方法で、Guard モジュールでゾーン保護をアクティブにできます。

- 手動：Guard モジュールに手動でアクセスし、ゾーンの保護をアクティブにできます。
- 自動：ネットワーク攻撃検出デバイス（Cisco Traffic Anomaly Detector（Detector）など）からの保護アクティベーション メッセージを受け入れるように Guard モジュールを設定できます。

（注）　Detector は、Guard モジュールの関連製品です。Detector は、DDoS 攻撃を検出するデバイスで、ゾーン トラフィックのコピーを分析し、ゾーンが攻撃を受けていると判断すると Guard モジュールの攻撃軽減サービスをアクティブにできます。また、Detector は Guard モジュールとゾーン設定を同期させることができます。Detector の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』および『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

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
- さまざまな保護モードについて
- 保護およびラーニング機能について
- オンデマンド保護について
- 攻撃レポートについて

トラフィック フィルタについて

Guard モジュールは、4 種類のトラフィック フィルタを使用して、必要な保護レベルをゾーン 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 保護操作を制御するように設定できます。

Guard モジュールでは、次のタイプのフィルタが使用されます。

- ユーザ フィルタ：必要な保護レベルを指定されたトラフィック フローに適用します。
- バイパス フィルタ：Guard モジュールが特定のトラフィック フローに DDoS 保護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 フローをカウントまたはドロップします。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：指定されたトラフィック フローに必要な保護レベルを適用します。Guard モジュールは、ゾーンに対する攻撃を検出したときにだけ動的フィルタを作成し、トラフィック フローの分析に基づいて動的フィルタを設定します。Guard モジュールは、ゾーン トラフィック、DDoS 攻撃のタイプ、および攻撃特性の変化に基づいて、このフィルタ セットを常に変更します。

Guard モジュールには次の 3 つの保護レベルがあり、各レベルでさまざまなプロセスをトラフィック フローに適用できます。

- 分析保護レベル：トラフィックの通過を許可します。ゾーン保護中、通過するトラフィックは、監視された状態ですが、異常が検出されない限り遮断されません。Guard モジュールは、異常を検出すると、適切な保護レベルをそのトラフィックに適用します。
- 基本保護レベル：スプーフィング防止機能やゾンビ防止機能をアクティブにし、疑わしいトラフィック フローを調べてトラフィックを認証し、その送信元を確認します。

- 強化保護レベル：強力なスプーフィング防止機能をアクティブにします。この機能により、トラフィック フローのパケットが調べられ、その正当性が確認されます。

Guard モジュールはトラフィックを分析し、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。また、ゾーンに注入するトラフィックのレートを制限し、トラフィック フローが一杯にならないようにします。

フィルタの詳細については、第 7 章「ゾーンのフィルタの設定」を参照してください。

さまざまな保護モードについて

次の方法で、Guard モジュールをアクティブにしてゾーン保護を行うことができます。

- 自動保護モード：攻撃中に作成する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：攻撃中に動的フィルタを作成します。ただし、動的フィルタをアクティブにはしません。代わりに Guard モジュールは、推奨されるアクションを受け入れるか、無視するか、または自動アクティベーションに切り替えるかどうかをユーザが確認および決定できるように、推奨されるアクションとして動的フィルタをグループ化します。

保護モードの詳細については、第 11 章「インタラクティブ保護モードの使用方法」を参照してください。

保護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保護を同時にアクティブにして（保護およびラーニング機能）、ゾーン ポリシーのしきい値のラーニングとトラフィック異常の監視を Guard モジュールが同時に行うようにできます。Guard 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、攻撃の軽減を開始します。攻撃が終了すると、Guard モジュールはラーニング プロセスを再開します。このプロセスにより、Guard 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。

保護およびラーニング機能の詳細については、P.9-14 の「保護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。

オンデマンド保護について

デフォルトのゾーン テンプレートおよび関連付けられているデフォルト ポリシーを使用すると、Guard モジュールによるゾーン トラフィック特性のラーニングをイネーブルにしなくても、ゾーンを保護することができます。Guard モジュールのゾーン テンプレート内のデフォルトのポリシーとフィルタは、Guard モジュールにとって未知のトラフィック特性を持つゾーンを保護できます。

オンデマンド保護の詳細については、P.10-3 の「オンデマンド保護のアクティブ化」を参照してください。

攻撃レポートについて

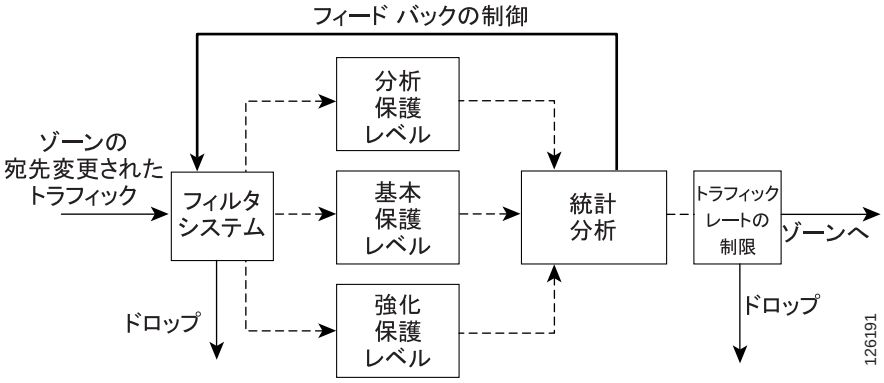
Guard モジュールは、各ゾーンの攻撃レポートを提供します。攻撃レポートでは、最初の動的フィルタの生成から保護の終了まで、ゾーンのステータス情報と攻撃の詳細な情報が提供されます。

攻撃レポートの詳細については、第 12 章「攻撃レポートの使用方法」を参照してください。

保護サイクルについて

Guard モジュールの保護サイクルは、ゾーン フィルタ、ゾーン ポリシー、およびトラフィック フローに対する Guard の保護レベルに適用され、ゾーン トラフィックを分析してクリーンにし、正当なトラフィックのみをゾーンに戻します。図 1-2 に Guard モジュールの保護サイクルを示します。

図 1-2　Guard の保護サイクル



手動でまたは Detector などの異常検出デバイスによってゾーン保護がアクティブにされると、Guard モジュールはゾーン トラフィックを自分宛に宛先変更し、ゾーン設定のポリシーによってトラフィック フローを監視します。ポリシーは、特定のトラフィック フローがポリシーのしきい値を超過すると、そのフローに対してアクションを実行します。ポリシー アクションは、通知の発行から、新しいフィルタ（動的フィルタ）の作成にまで及びます。このフィルタは、トラフィックを適切な保護レベルに転送するものです。Guard モジュールはトラフィック フローを分析し、ゾーンで対応可能な定義済みのレートを超えたトラフィックをドロップし、正当なトラフィックをゾーンに戻します。

攻撃中、Guard モジュールは、クローズド ループのフィードバック サイクルを実行します。このサイクルで、Guard は、動的に変化するゾーン トラフィック特性に合せてゾーン保護措置を調整します。Guard モジュールは、保護戦略を調整し、DDoS 攻撃やトラフィック フローの変化に対応します。事前定義された期間中に、使用されている動的フィルタがなく、ゾーンへのトラフィックがドロップされず、新しい動的フィルタが追加されなかった場合、Guard モジュールはゾーン保護を停止します。

1 Gbps と 3 Gbps の帯域幅オプションについて

Guard モジュールは、1 Gbps（ギガビット / 秒）または 3 Gbps の 2 つの帯域幅パフォーマンスレベルで動作可能です。Guard モジュールにロードしたソフトウェア イメージにより、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が制御され、動作帯域幅が決まります。インストールされたソフトウェア イメージにより、次のようにインターフェイスが制御されます。

- 6.0 ソフトウェア イメージ : スループットは 1 Gbps で、データ トラフィックは 1 つのインターフェイス ポートを経由してスーパーバイザ エンジンと Guard モジュールの間を移動できます。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のみを転送します。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 : スループットは 3 Gbps で、3 つのインターフェイス ポートすべてがデータ トラフィックとインバンド管理トラフィックを転送できます。各ポートの最大帯域幅は 1 Gbps で、動作の合計帯域幅は 3 Gbps になります。XG ソフトウェア イメージを使用するには、Guard モジュールでソフトウェア ライセンスが必要になります。

（注）　ソフトウェア イメージがインストールされた Guard モジュールを注文するか、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（3 Gbps 動作）にアップグレードできます。6.0-XG ソフトウェア イメージを含む新しい Guard モジュールを注文する場合は、シスコがソフトウェア イメージとともに必要なライセンスをインストールします。6.0-XG ソフトウェア イメージへのアップグレードについては、P.14-19 の「1 Gbps から 3 Gbps への帯域幅のアップグレード」を参照してください。

表 1-1 に、Guard モジュールの物理インターフェイスとスーパーバイザ エンジン ポート間の相関を示します。表には、3 Gpbs 動作対応のソフトウェア イメージをインストールした後に、インターフェイス eth1（管理トラフィックのみ）の CLI 指定子が giga1（データおよび管理トラフィック）に変更されるしくみも示しています。

表 1-1　スーパーバイザ エンジンのポートおよび相関する Guard モジュールのインターフェイス

スーパーバイザ エンジン ポート	Guard モジュール 1 Gbps 動作		Guard モジュール 3 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	eth1	管理 (アウトオブバンド)	giga1	データおよびインバンド管理
ポート 2	giga2	データ	giga2	データおよびインバンド管理
ポート 3	giga3	未使用	giga3	データおよびインバンド管理

次の項目は、1 Gbps 動作と 3 Gbps 動作とのインターフェイス設定の違いを説明しています。

- Guard モジュールの物理インターフェイスへの IP アドレスの割り当て :
  - 1 Gbps 動作 : IP アドレスを giga2 にのみ割り当てます。
  - 3 Gbps 動作 : 固有の IP アドレスを各インターフェイスに割り当てます（アドレスは同じサブネット上に存在する必要があります）。
- Guard モジュールの物理インターフェイス上でのプロキシの設定 :
  - 1 Gbps 動作 : 1 つ以上のプロキシを giga1 でのみ設定します。

  - 3 Gbps 動作：1 つ以上のプロキシを各インターフェイスで設定します。
- スーパーバイザ エンジンでのデータ トラフィック VLAN の設定：
  - 1 Gbps 動作：データ トラフィック VLAN をポート 2 でのみ定義します。
  - 3 Gbps 動作：データ トラフィック VLAN をスーパーバイザ エンジンの 3 つのポートすべてで定義します。
- Guard モジュールでのデータ トラフィック VLAN の設定：
  - 1 Gbps 動作：VLAN を giga2 物理インターフェイスでのみ定義します。
  - 3 Gbps 動作：VLAN を Guard モジュールの 3 つの物理インターフェイスすべてで定義します。
- スーパーバイザ エンジンでの管理トラフィック VLAN の設定：
  - 1 Gbps 動作：アウトオブバンド管理トラフィックの VLAN をポート 1 でのみ定義します。
  - 3 Gbps 動作：アウトオブバンド管理トラフィックの VLAN を 1 つ以上のポートで定義します。
- Guard モジュールでの管理トラフィック VLAN の設定：
  - 1 Gbps 動作：アウトオブバンド管理トラフィックの VLAN をインターフェイス eth1 でのみ定義します。
  - 3 Gbps 動作：インバンド管理トラフィックの VLAN を 1 つ以上の物理インターフェイスで定義します。

3 Gbps ソフトウェア イメージで動作させる場合、Guard モジュールは、ユーザがゾーン保護をアクティブにするときにインターフェイス設定を確認します。3 つのインターフェイスがトラフィックの宛先変更を行うように適正に設定されていない場合、Guard モジュールはゾーン保護をアクティブにしません。Guard モジュールはまた、インターフェイス設定モードに入る場合、プロキシ IP アドレスを削除する場合、またはトラフィックの宛先変更パラメータを設定する場合に、確認プロセスを手動でアクティブにすることを要求します。確認プロセスの詳細については、P.5-23 の「Guard モジュールのネットワーク設定の検証」を参照してください。