CHAPTER 1

製品概要

この章では、Cisco Guard（Guard）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。

この章には、Guard の関連製品である Cisco Detector（Detector）についての記述があります。Detector とは、ゾーン トラフィックのコピーを分析する、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃検出デバイスのことです。Detector 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 は、ゾーンの設定を Guard と同期させることもできます。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。

この章は、次の項で構成されています。

Cisco Guard について

Cisco Guard（Guard）は、有効な DDoS 攻撃軽減デバイスで、疑わしいトラフィックを宛先変更して処理し、攻撃パケットをドロップし、正当なトランザクションを転送します。

Guard は、ネットワーク要素であるゾーンを DDoS 攻撃から保護します。Guard は、攻撃対象から宛先変更されたトラフィックを受信し、特定の攻撃パケットを識別して削除し、正当なトラフィックを元の宛先に転送します。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。

通常 Guard 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 は攻撃を検出すると、攻撃されたゾーンのトラフィックのみを自分宛に宛先変更します。他のゾーンのトラフィックは、遅れることなくそのまま流されます。Guard はパケットを分析して DDoS コンポーネントを除去し、クリーンなトラフィック パケットが目的のゾーンに流れるようにします。

Guard は常に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 には、次の機能があります。

- トラフィックの宛先変更メカニズム。このメカニズムにより、ゾーンのトラフィックがラーニング システムと保護システムに宛先変更され、その後正当なトラフィック フローがゾーンに戻されます。この機能がネットワーク トラフィックに支障をきたすことはありません。
- アルゴリズムに基づいたラーニング システム。このラーニング システムは、ゾーンのトラフィックをラーニングし、それ自体を特定の特性に適合させ、しきい値とポリシーという形で参考値と保護のための指示を与えることにより、保護プロセスをサポートします。また、Guard には、Guard がゾーンのトラフィックのラーニング プロセスとそのトラフィックに合せた調整を完了していないときにゾーンが攻撃された場合に対応するために、オンデマンドの保護も用意されています。
- 保護プロセス。このプロセスでは、正当なトラフィックと疑わしいトラフックが区別され、悪意のあるトラフィックがフィルタリングされ、正当なトラフィックのみがゾーンに渡されます。

Guard は、これらのコンポーネントを統合することにより、攻撃時には保護の役割を果たし、それ以外のときにはバックグラウンドに控えた状態を保つことができます。

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、攻撃者が制御するマスター サーバから、いつ、どのように組織的攻撃を開始するかの指示を受けます。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

Guard は、ゾーンのネットワーク アドレスの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。

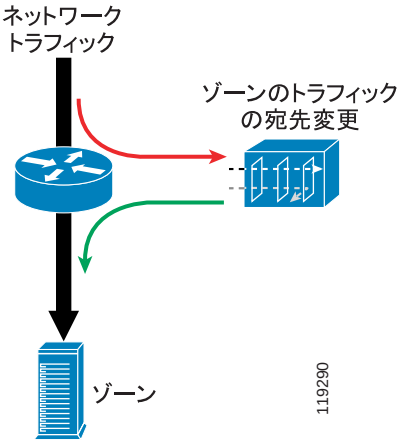
ゾーンを定義するときに、Guard がゾーンの保護に使用するネットワーク アドレスとポリシーを設定します。ゾーンに名前を割り当てて、この名前を使用してゾーンを参照します。

Guard の動作のしくみについて

ターゲット ホスト（ゾーン）を保護するために、Guard はゾーン トラフィックを自分自身に宛先変更します。外部（Cisco Traffic Anomaly Detector など）から攻撃の兆候が示されてから Guard を設定してゾーンを保護することも、ゾーンの設定完了後すぐにゾーンを保護するように Guard に指示することもできます。Guard はデータ フローを分析し、すべての DDoS 要素をブロックし、宛先変更されたストリームから悪意のあるパケットを除去し、クリーンなトラフィックが目的のゾーンに流れるようメインのデータ パスに戻します。図 1-1 に、保護動作を示します。

Guard のルーティング設定を使用して、トラフィックの宛先変更をグローバルに設定してください。詳細については、付録 A「ゾーン トラフィックの宛先変更について」を参照してください。

図 1-1　Cisco Guard の動作



Guard は、ゾーンのトラフィックの特性をラーニングして、ゾーンのトラフィックを比較し、悪意の攻撃となる可能性のある異常をすべてトレースします。

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

ネットワーク上に攻撃が発生していなくても、Guard のラーニング プロセスによって正常なトラフィック パターンのベースラインが作成されます。Guard はこれを、異常の発生を検出するための参照ポイントとして使用します。これらの参照ポイントをポリシーといいます。

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：Guard　は、ゾーンのポリシーを作成します。ポリシー テンプレートは、Guard 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 Guard を通過することにより、Guard は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：Guard は、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 Guard を通過することにより、Guard 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 Guard 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、Guard 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、Guard 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保護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。

Guard によるゾーン保護のしくみについて

Guard 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：動的フィルタは、自動でアクティブになります。
- インタラクティブ保護モード：Guard は、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 は、動的フィルタを推奨処置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、または自動アクティベーションに切り替え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

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）、Guard 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。Guard 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、ゾーン保護は継続します。このプロセスにより、Guard 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、Guard はラーニング プロセスを再開します。詳細については、P.8-21 の「ゾーンのポリシーのしきい値調整とゾーン保護のイネーブル化の同時実行」を参照してください。

オンデマンド保護について

システム定義のゾーン テンプレートを使用すると、Guard 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。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 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。詳細については、P.9-3 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 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。

保護プロセスについて

Guard は、ゾーンのトラフィックを必要な保護レベルに誘導するために、4 種類のフィルタを使用します。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 保護防止操作を制御するように設定できます。

Guard 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：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。
- バイパス フィルタ：Guard 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：指定されたトラフィック フローをカウントまたはドロップします。フレックスコンテンツ フィルタには非常に柔軟なフィルタリング機能があり、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が可能です。
- 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 は、トラフィック フロー分析に基づいて動的フィルタを作成します。Guard は、このフィルタ セットを常にゾーン トラフィックや DDoS 攻撃のタイプに合せて調整しています。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。

Guard 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 フローに適用しています。

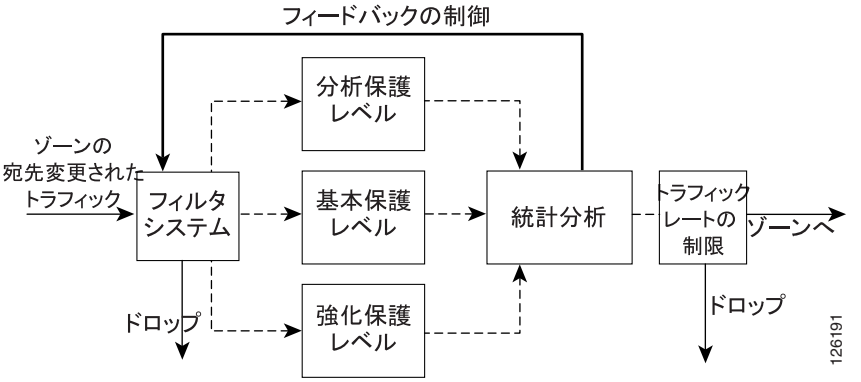
- 分析保護レベル：Guard はトラフィックを監視状態で流します。ただし、保護中に異常がトレースされていない場合、トラフィックは影響を受けません。Guard が異常をトレースすると、そのトラフィックを適切な保護レベルに誘導します。
- 基本保護レベル：Guard はスプーフィング防止機能やゾンビ防止機能をアクティブにし、疑わしいトラフィック フローを調べてトラフィックを認証し、その送信元を確認します。
- 強化保護レベル：Guard は、強力なスプーフィング防止機能をアクティブにします。この機能により、トラフィック フローのパケットが調べられ、その正当性が確認されます。

Guard 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。

保護サイクルについて

Guard 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、ゾーンをクリーンにして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 の保護サイクルを示します。

図 1-2　Guard の保護サイクル



ゾーン保護がアクティブになると、ゾーン ポリシーによりゾーンのトラフィック フローが監視されます。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。実行するアクションは、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、宛先変更されたトラフィックを関連する保護レベルに誘導するものです。Guard は、いくつかの認証方式を使用してトラフィックを認証します。Guard 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。

Guard は、クローズド ループのフィードバック サイクルを制御して、動的に変化するゾーン トラフィック特性に合せて Guard の保護処置を調整します。Guard は適切な保護戦略を採用し、次々に変化する DDoS 攻撃のタイプやトラフィック フローに対応します。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 はゾーン保護を停止します。