概要

この章では、Cisco Anomaly Guard Module（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、次の項があります。

DDos について

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃は、悪意のある個人が、セキュリティを侵された数千台ものコンピュータ（ゾンビ）に自動化されたスクリプトを実行させて偽のサービス要求を発行し、保護されたサーバ（ゾーン）のネットワーク リソースを使用不能にする攻撃です。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消費者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。ゾンビは、多くの場合、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ものは、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、大企業も含めた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。

DDoS 攻撃は統計的な現象であるため、詳細で統計的なトラフィック プロファイルの形成が必要になります。DDoS の調査では、DDoS のゾンビは自律システム内に多数分散していること、正当なサービス要求と偽のサービス要求が密に統合されていること、および、DDoS 攻撃ではランダムな設定（IP 送信元アドレスのスプーフィングや TCP フラグのランダム設定など）が使用されていることなどが指摘されています。

高度な知識を持ったハッカーは、攻撃用の新たな不正手段を生み出し続けており、DDoS 攻撃は常に進化しています。また、これらの攻撃スクリプトはインターネット上で容易に入手でき、ネットワークに関する技術知識があまりない人物がごく普通に実行しています。このため、DDoS 防御テクノロジーは柔軟かつ臨機応変なものである必要があります。

つまり、DDoS 防御システムは、近づく DDoS 攻撃を検出し、悪意のあるトラフィックと正常なトラフィックを区別し、攻撃対象となっているネットワーク要素のトラフィック フローを妨げることなくこれらのタスクを実行できるものである必要があります。

Cisco Anomaly Guard Module

Cisco Anomaly Guard Module（Guard モジュール）は Cisco IOS アプリケーション モジュールの 1 つで、次の製品のどちらかに設置できます。

- Supervisor Engine 720（SUP720）、または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を備えた Supervisor Engine 2（SUP2）が搭載された、Cisco Catalyst 6500 シリーズ スイッチ
- SUP720 が搭載された Cisco 7600 ルータ

このサービス拒絶（DoS）軽減製品は、攻撃対象から宛先変更されたトラフィックを受信して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。この製品は、分散型のアップストリーム構成に ISP、MSP、またはバックボーン レベルで導入され、ネットワーク全体を保護します。攻撃が検出されると、攻撃対象ゾーンのトラフィックのみが宛先変更され、Guard に送られます。また、データ フローが分析されます。すべての DDoS コンポーネントは除去され、クリーンなトラフィックが継続して目的のゾーンへ流されます。Guard は、トラフィックを常時フィルタリングしながらゾーンの透過的なトラフィック フローを可能にし、新たに発生する攻撃パターンに備えるために、常にゾーンのトラフィック特性に合せて調整された状態を保ちます。

このような動作を行うために、Guard では、次のコンポーネントが使用されています。

- 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 Guard のラーニング システムと保護システムにリダイレクト（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（注入され）ます。この処理は、ネットワーク トラフィックを妨げることなく実行されます。
- 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、保護システムをサポートします。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。
- 正当なトラフィックと疑わしい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する保護システム。フィルタリング後は、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。攻撃の疑いがない場合は、宛先変更プロセスをアクティブにする必要はなく、Guard モジュールはトラフィックを監視しません。

ゾーンについて

ゾーンは、Guard モジュールが DDoS 攻撃からの保護対象とするネットワーク要素です。

ゾーンは、ネットワーク サーバ、クライアント、ルータ、ネットワーク リンク、サブネット、ネットワーク全体、個々のインターネット ユーザ、企業、インターネット サービス プロバイダー（ISP）、またはこれらを組み合せたものを包含できます。

Guard モジュールは、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。

Guard モジュールは、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、複数のゾーンのトラフィックを同時に分析できます。

ゾーンはネットワーク要素の定義で、Guard モジュールはこの設定されたゾーンを DDoS 攻撃から保護することができます。

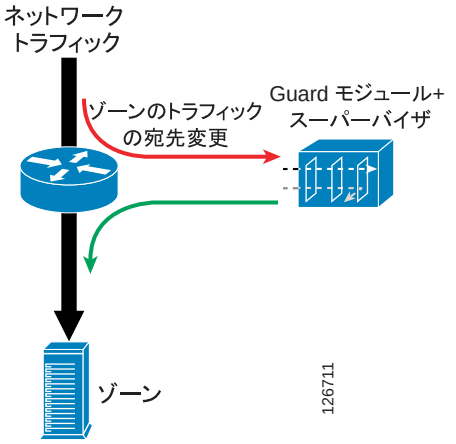
この定義は、ネットワーク アドレスや検出ポリシーなどの設定で構成されます。ゾーンに名前を割り当てて、この名前でゾーンを参照することができます。

Guard モジュールの動作のしくみについて

ターゲット ホスト（ゾーン）を保護するには、そのホストへのトラフィックが宛先変更され、Guard モジュールに送られる必要があります。外部（Cisco Traffic Anomaly Detector Module やその他の手段）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 フローを分析します。すべての DDoS 要素はブロックされ、宛先変更されたストリームから悪意のあるパケットが除去されます。クリーンなトラフィックはメインのデータ パスに戻され、目的のゾーンに継続して流されます。図 1-1 に、保護動作の概要を示します。

宛先変更は、Guard モジュールのルーティング設定を通じてグローバルに設定されます。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

図 1-1　Cisco Anomaly Guard Module の動作



ゾーンのトラフィックを比較する際の基準を作り、悪意の攻撃となる可能性のあるあらゆる異常をトレースするために、Guard はゾーンのトラフィックの特性をラーニングします。

また、ゾーンが攻撃にさらされている場合などは、必要に応じて、ラーニング プロセスを実行せずにゾーンを保護することもできます。システム定義のゾーン テンプレートには、ラーニング プロセスが完了していないゾーンの保護に適した定義済みの保護ポリシーとフィルタが含まれています。詳細については、P.6-45 の「オンデマンド保護のイネーブル化」を参照してください。

ラーニング プロセスは次の 2 つのフェーズで構成されます。これらのフェーズで Guard はゾーンのトラフィックをラーニングし、特定の特性に対応します。

1. **ポリシー構築フェーズ**：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、ポリシーの構築に使用される規則を提供します。トラフィックが透過的に Guard を通過し、Guard はゾーンによって使用される主なサービスを検出できます。
2. **しきい値調整フェーズ**：ゾーンのサービスのトラフィック レートに合せてポリシーを調整します。トラフィック フローは Guard をそのまま通過し、Guard はポリシー構築フェーズで検出されたサービスに使用するしきい値を調整します。

しきい値調整フェーズをアクティブにし、さらにゾーン保護も同時にアクティブにすることができます。この動作状態では、Guard モジュールは、ゾーン ポリシーのしきい値をラーニングし、同時にトラフィックの異常に関するポリシーのしきい値を監視することができます。Guard モジュールは攻撃を検出すると、ラーニング プロセスを停止しますが、ゾーン保護は継続します。この結果、Guard 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、Guard モジュールはラーニング プロセスを再開します。

ポリシーは、Guard モジュール統計エンジンの構成要素です。各ゾーンには、ゾーンのトラフィック パターンに合せて調整されたポリシーのセットがあります。これらのポリシーは、悪意となる可能性のある異常をトレースするために、Guard モジュールがゾーンのトラフィックと比較する基礎となります。ポリシーは、トラフィック フローを持続的に測定し、特定のトラフィック フローが悪意のあるものまたは異常であると判断すると、そのフローに対してアクションを実行します。このアクションは、フローがポリシーのしきい値を超過すると発生します。

トラフィックのラーニングの詳細については、第 6 章「ゾーンの設定」を参照してください。ゾーンの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。

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、Guard はそのトラフィックを悪意のあるものまたは異常であると識別します。そして一連のフィルタ（動的フィルタ）を動的に設定し、そのトラフィックを攻撃の重大度に従って適切な保護モジュールに誘導します。

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：動的フィルタはユーザの操作なしでアクティブになります。
- インタラクティブ保護モード：動的フィルタは、手動でインタラクティブにアクティブになります。動的フィルタは推奨事項としてグループ化され、ユーザの決定を待ちます。ユーザは、これらの推奨事項を確認して、どの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できます。

詳細については、第 9 章「インタラクティブ保護モード」を参照してください。

Guard は、ゾーンのステータスを明確につかめるようにするために、すべての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、攻撃の詳細な情報が提供されます。

詳細については、第 10 章「攻撃レポート」を参照してください。

保護のメカニズム

Guard の保護システムでは、次のメカニズムが使用されます。

- フィルタ
- 保護モジュール

フィルタ

ゾーンのフィルタは、宛先変更されたトラフィックを関連する保護モジュールに誘導します。Guard では、ユーザがフィルタを設定して、カスタマイズされたトラフィック誘導や DDoS 攻撃の防止メカニズムをさまざまに設計できるようになっています。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 フローを関連する Guard の保護モジュールに誘導します。
- バイパス フィルタ：特定のトラフィック フローが Guard の保護メカニズムによって処理されないように防止します。
- フレックスコンテンツ フィルタ：指定されたパケット フローをカウントまたはドロップします。フレックスコンテンツ フィルタは、バークリー パケット フィルタとパターン フィルタを組み合せたもので、IP ヘッダーと TCP ヘッダーのフィールドに基づいたフィルタリングやコンテンツのバイト数に基づい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をユーザに提供します。
- 動的フィルタ：指定されたトラフィック フローを関連する Guard の保護モジュールに誘導します。Guard は、トラフィック フローを分析した結果として動的フィルタを作成します。この一連のフィルタは、ゾーンのトラフィックおよび特定の DDoS 攻撃に合せて継続的に調整されます。動的フィルタは有効期間が限定されており、攻撃が終了すると消去されます。

保護モジュール

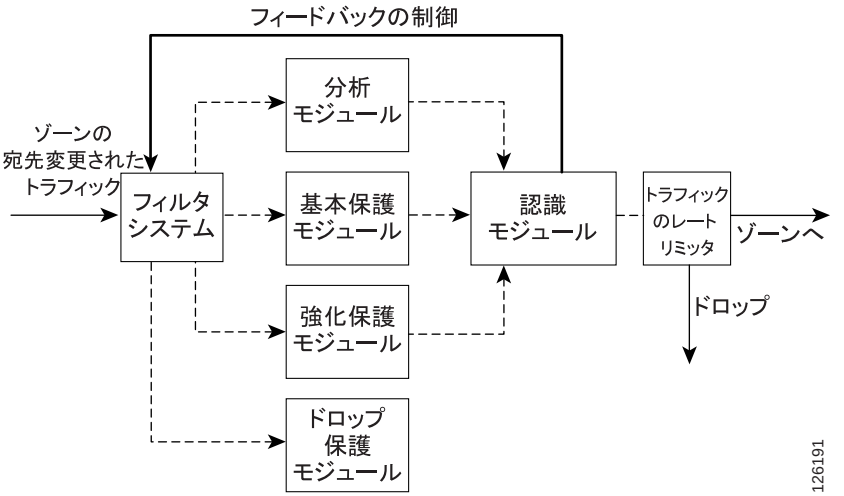
Guard モジュール の保護モジュールは、トラフィック フローにさまざまなプロセスを適用します。Guard には、次の保護モジュールがあります。

- 分析保護モジュール：この保護モジュールにより、トラフィックを監視状態で流すことができます。ただし、保護中も異常がトレースされていない間はトラフィックは影響を受けません。異常がトレースされると、トラフィック フローは適切な保護モジュールに誘導されます。
- 基本保護モジュール：この保護モジュールは、トラフィックを認証するスプーフィング防止メカニズムとゾンビ防止メカニズムを提供します。これらのメカニズムは、疑わしいトラフィック フローを検査し、その送信元を確認します。
- 強化保護モジュール：この保護モジュールは、より強力なスプーフィング防止メカニズムを備えています。これらの認証メカニズムは、フローのパケット検査し、フローの正当性を確認します。
- ドロップ保護モジュール：この保護モジュールは、悪意のあるトラフィックをドロップします。
- レート リミット保護モジュール：この保護モジュールは、目的のトラフィック フローまたはゾーン トラフィック全体のレートを制限します。
- 認識および統計保護モジュール：この保護モジュールは、ポリシーとフィルタ システム間の調整を行います。ゾーンのポリシーを適用し、ゾーンのトラフィックの異常を監視します。

保護サイクル

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、Guard のポリシーはゾーンのトラフィック 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。ポリシーが実行するアクションは、単なる通知の発行から、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モジュールに誘導します。保護モジュールは、このトラフィックを認証します。サンプルでは、トラフィックは認識保護モジュールに流れています。このモジュールでは、ゾーンのポリシーを適用し、ゾーンのトラフィックの異常を監視します。

Guard は、ゾーンに流れるトラフィックのレートを監視します。定義済みのレートを超過するトラフィックはドロップされ、正当なトラフィックはゾーンに転送されます。Guard は、ゾーンのトラフィックの統計分析を行い、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のトラフィック特性や変化する DDoS 攻撃のタイプに合せて保護措置を調整します。

Guard は、使用されている動的フィルタがなくなり、ゾーンへのトラフィックがドロップされず、事前に定義された期間で新しい動的フィルタが追加されなかった場合に、ゾーン保護を停止します。