概要

この章では、Cisco 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 とは

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、何千もの信頼のおけないコンピュータ（「ゾンビ」）に自動化されたスクリプトを実行させ、保護されたサーバ（ゾーン）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できなくする攻撃です。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）サーバの可用性と正確性を損なわせようと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。

DDoS 攻撃は、高度な技術を持つハッカーが新しい有害なプログラムを作成するのに伴い、進化を続けています。さらに、ハッカーによる攻撃スクリプトは、インターネット上で広く使用可能になっており、ネットワーキングに最低限の技術的知識しか持たない個人によって日常的に実行されています。したがって、DDoS 防御テクノロジーは、柔軟で適応力のある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 Guard

Cisco Guard は、ハイ パフォーマンス ネットワーク デバイスです。

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そのトラフィックをクリーンにし、元のパスに転送します。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わ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、Cisco 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ます（注入）。この動作は、ネットワークのトラフィックに支障をきたす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とそのトラフィックに合わ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 はトラフィックを監視しません。

ゾーン

ゾーンは、Guard が DDoS 攻撃からの保護対象とするネットワーク要素です。ゾーンには、ネットワーク サーバ、クライアントやルータ、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 ユーザや企業、インターネット サービス プロバイダー（ISP）、およびこれらのあらゆる組み合せが考えられます。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。

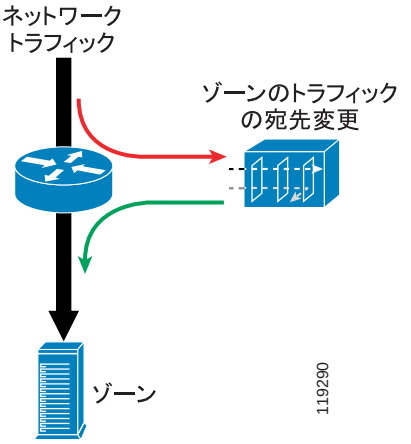
ゾーンはネットワーク要素の定義で、Guard はこの設定されたゾーンを DDoS 攻撃から保護することができます。ゾーンには、名前を割り当て、この名前を使用してゾーンを参照します。

Guard の動作のしくみ

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 に送られる必要があります。外部（Cisco Detector 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 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、付録 A「宛先変更の設定」を参照してください。

図 1-1　　Cisco Guard 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.5-20 の「オンデマンド保護」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、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**：このフェーズでは、Guard のポリシー テンプレートを使用して、ゾーンのポリシーが作成されます。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、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**：このフェーズでは、ゾーンのサービスのトラフィック レートに合わせてポリシーが調整されます。トラフィックが透過的に Guard を通過し、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。

ポリシーは、特定のトラフィック フローを測定し、しきい値の超過があった場合にそのフローに対してアクションを実行するメカニズムです。保護ポリシーは、ポリシー テンプレートから構築されます。

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。ゾーンの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 のポリシーが（しきい値の超過によって）異常なトラフィックや悪意のあるトラフィックを検知すると、ポリシーは動的に一連のフィルタ（動的フィルタ）を設定して、そのトラフィックを攻撃の重大度に従って適切な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　モード：動的フィルタは、手動で対話的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、受け入れ、無視、または自動的なアクティブ化を決定します。

詳細については、第 8 章「インタラクティブ推奨モード」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 9 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

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：ユーザ フィルタは、特定のトラフィック フローを関連する Guard の保護モジュールに誘導する場合に使用されます。
- バイパス フィルタ：バイパス フィルタは、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する場合に使用されます。
- フレックス フィルタ：フレックス フィルタは、指定したパケット フローのカウントまたはドロップに使用されます。これは、IP および TCP ヘッダーのフィールドに従ったフィルタリングや、コンテンツのバイト数に従ったフィルタリングのように、きわめて柔軟なフィルタ機能を提供するバークリー パケット フィルタです。複雑なブール式を使用できますが、フレックス フィルタを設定できるのはゾーンごとに 1 つだけです。
- 動的フィルタ：トラフィック フローの分析の結果、Guard によって作成される動的なフィルタです。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 攻撃に合わせて継続的に調整されます。動的フィルタは継続期間が限定されており、攻撃が終了すると消去されます。

モジュール

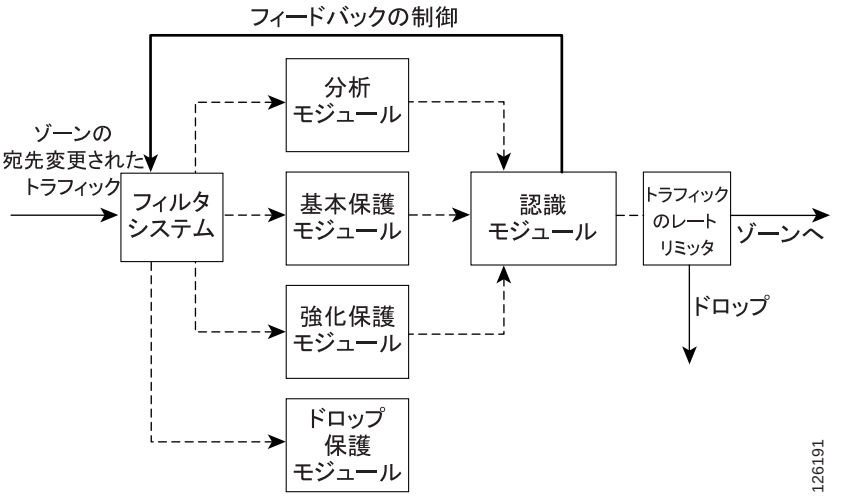
Guard の保護モジュールは、トラフィック フローにさまざまなプロセスを適用します。Guard には、次の保護モジュールがあります。

- 分析モジュール：このモジュールにより、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。
- 基本モジュール：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。
- 強化モジュール：より厳格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 モジュール：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 モジュール：目的のトラフィック フローまたはゾーン トラフック全体のレートを制限します（詳細については、P.6-12 の「バイパス フィルタの設定」を参照）。
- 認識モジュール：Guard のポリシーとフィルタ システム間の調整を行います。

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



保護がアクティブになると、Guard はゾーンのトラフィックを宛先変更します。Guard のポリシーは、トラフィック フローを測定し、しきい値の超過があった特定のトラフィック フローに対してアクションを実行します。実行されるアクションは、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モジュールに流れています。Guard は、トラフィックをレート リミッタに渡します。定義されたレートを超過するトラフィックは、ここでドロップされます。クリーンになったトラフィックは、再びゾーンに注入されます。

認識モジュールは、クローズド ループのフィードバック サイクルを制御して、Guard の保護措置を動的に変化するゾーンのトラフィック特性に合わせて調整します。Guard は、適切な保護方針を適用して、変化する DDoS 攻撃のタイプとトラフィック フローに対応します。Guard は、使用されている動的フィルタがなくなり、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、保護を停止します。