あらゆる規模・タイプのDDoS攻撃に対応する検知、分析、防御機能

A10 NetworksとFlowmon Networksの統合ソリューションでネットワークトラフィックの監視とDDoS攻撃の制御を実現

課題：

ネットワークを保護するには、組織のサービスとインターネットを往来するトラフィックフローから詳細な洞察が必要です。ヒストリカルデータと最新のデータに基づいてネットワークリソースを拡張し、アルゴリズムを駆使してサービス可用性を脅かす異常を検出することは管理者にとって有効な情報になります。

ソリューション：

Flowmonでは、ネットワーク内の詳細な情報と統計情報が提供されます。DDoS攻撃などネットワークの異常が検出されると、FlowmonとA10 Thunder TPSの連携によって疑わしいトラフィックがリダイレクトされて詳細に分析し検査されるため、どんなに規模が大きく、巧妙なDDoS攻撃であっても制御できます。

利点：

- Flowmonでは、ネットワークトラフィックフローから深い洞察が提供できます。
- DDoSの検出と防御が自動化されているため、疑わしいトラフィックはA10 Thunder TPSに自動的に転送されて、詳細な検査とDDoS緩和策が実行されます。
- ネットワークトラフィックは継続的に監視および分析されて、正常な状態のベースラインが確立され、ネットワークの異常を即座に検出します。

Flowmon
Driving Network Visibility

インテリジェンスとパフォーマンス

ネットワークトラフィック管理はさまざまな課題に直面しています。分散サービス妨害（DDoS）攻撃ではハクティビズムによる主義主張、恐喝、あるいは単純な興味本位ないたずらまで、さまざまな動機から意図的に生成された悪意のあるトラフィックによってオンラインサービスが妨害されます。

ネットワークを管理するスタッフにとって、ネットワークトラフィックの状態、関連するトラフィックの種類、ネットワーク通信の発生元に関する情報は重要です。そのような情報は、ネットワークの拡張の必要性を予測したり、ネットワークの問題を分析するときにも活用できます。

DDoS攻撃のようなネットワークの問題はさまざまな形で起こります。一般的に大量のパケット数や帯域幅を消費する攻撃を想定しますが、そのような単純なDDoS攻撃だけではなく、同時にアプリケーション層を含めたマルチベクトル型のDDoS攻撃も増えてきています。

ネットワークフローのサンプルを解析すると、パケット数と帯域幅から幅広くネットワークを分析でき、深い洞察、高い可視性、複雑なネットワークインフラストラクチャを理解する上で価値のある情報を得ることができます。1秒間に大量のパケットを送信するDDoS攻撃など、トラフィックの異常を検出したら、次に問題になるのは、サービスが停止して組織の収益と評判が危険にさらされる前に攻撃を阻止する方法です。DDoS攻撃は多くの場合、複数のタイプのDDoS攻撃が並行して行われるため、DDoS対策ソリューションはあらゆるタイプのDDoS攻撃に対応する必要があります。このようなマルチベクトル型DDoS攻撃では、ネットワーク層やインフラストラクチャ層を攻撃するSYNフラッドやアプリケーション層を狙った攻撃が同時に行われます。ファイアウォールや侵入検知システム（IDS）デバイスなどの従来型のセキュリティソリューションでは、そのステートフルな性質からDDoS攻撃によって簡単に機能不能になるため、複数の種類のDDoS攻撃を同時に行なうようなマルチベクトル攻撃からネットワーク全体を保護するDDoS専用の対策ソリューションが必要になります。

A10とFlowmon

A10 NetworksはFlowmon Networksと提携し、フローベースのネットワークの洞察、分析およびDDoS対策機能を備え、柔軟性と拡張性に優れた低価格のソリューションを提供しています。Flowmonではネットワークを通過するトラフィックを監視し、ネットワークのさまざまなルータからフローのサンプルを受信して、トラフィックのベースラインが形成されます。ネットワークの異常が検出されると、A10のRESTful APIインターフェイスを介して、FlowmonからA10 Networks® Thunder TPS™脅威防止システムに攻撃の対象と必要な対策が通知されます。A10 Thunder TPSデバイスからは、不正なトラフィックをThunder TPSにリダイレクトするようネットワークに指示が送られます。トラフィックがリダイレクトされると不正なパケットが除去され、正規のトラフィックがターゲットサーバーに転送されます。

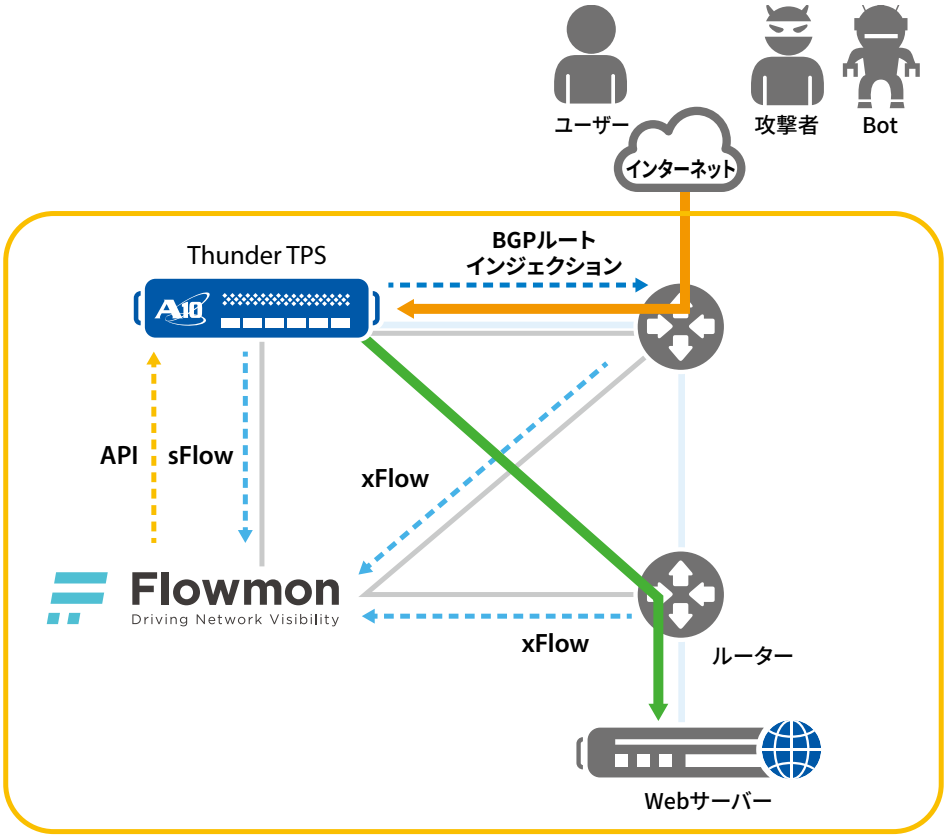

図 1：Thunder TPS と Flowmon の連携

管理と拡張の簡略化

Flowmon を使用すると、ネットワーク管理者やネットワークセキュリティ担当者はネットワークトラフィックを深く分析し、特定のトラフィックタイプやトラフィックレートに対するポリシーを定義できます。Flowmon は、ネットワークのトラフィックレートと固有のフローのサンプルレートに合わせてシームレスに拡張できます。また、直観的なインターフェイスによって、Flowmon で測定可能なさまざまなトラフィックパターンを表示できます。

Flowmon では、宛先 IP アドレスのベースラインが自動的に作成されます。それによって宛先に対する正規のトラフィックパターンが特定されて、トラフィックパターンの異常が判断されます。異常なトラフィックが検出されると、Thunder TPS によって不正なトラフィックをブロックする緩和ポリシーが適用されます。

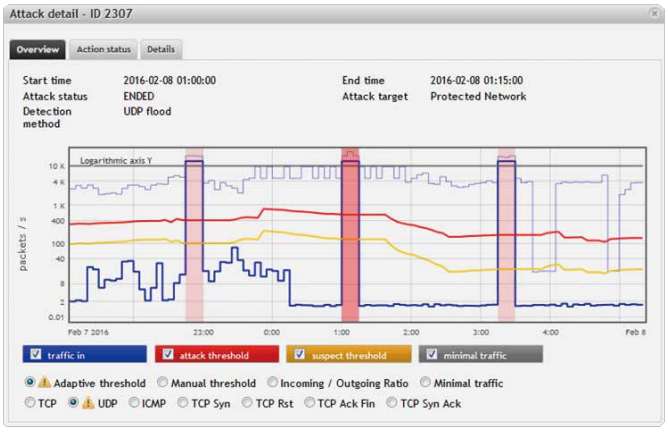

図 2：UDP フラッドの検出

A10 の Thunder Security and Policy Engine（SPE）を搭載した Thunder TPS モデルを選択すると、ハードウェアでトラフィック処理が加速されます。ハードウェアの処理で加速されると、Thunder TPS で 60 以上の単純な攻撃パターンをハードウェアで阻止するだけでなく、CPU リソースをより複雑なタスクに割り当てることができ、パフォーマンスを最大限に発揮しながら複雑なマルチベクトル型の攻撃も処理します。

機能と利点

Flowmon と Thunder TPS の統合ソリューションを使用すると、ネットワークトラフィックパターンを分析し、その分析で得た洞察を活用して DDoS 攻撃から保護することができます。Thunder TPS と Flowmon の統合ソリューションを導入すると、以下の利点が実現します。

- 深いトラフィック分析：Flowmon によってあらゆるレベルのネットワークトラフィックフローの洞察が提供されます。
- 検出と防御の自動化：疑わしいトラフィックは Thunder TPS に自動的に転送され、詳細に検証されて DDoS が阻止されます。Flowmon では通常のネットワークパターンが分析され、異常を自動的に検知します。その後、Thunder TPS によってボリューム攻撃とアプリケーション層を狙った攻撃の両方の DDoS トラフィックをすばやく除去します。
- リアクティブモデル：Flowmon と Thunder TPS を使用すると、動的でリアクティブな導入モデルが提供できます。Flowmon ではトラフィックが継続的に監視され、ベースラインから異常を検出した時に Thunder TPS に転送されるため、レイテンシーへの影響を最小限にします。

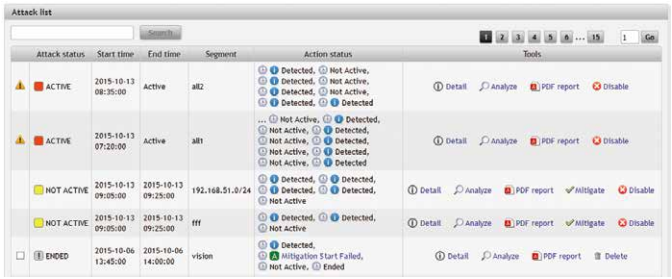

図3：DDoSの検出 (Flowmon DDoS Defender)

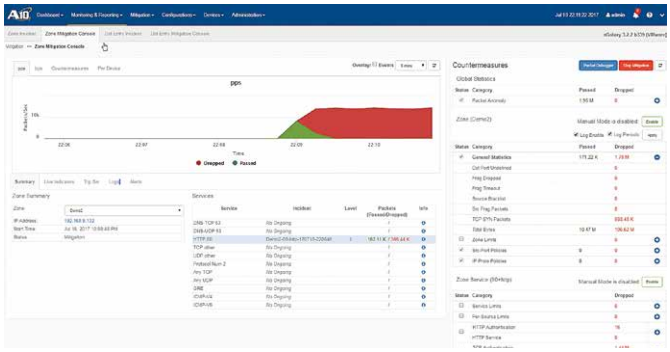

図4：DDoSの防御 (A10 Thunder TPS)

Flowmon Networks社について

革新的なフローベースのネットワーク監視とセキュリティのソリューションを提供するFlowmon Networks a.s.（Flowmon社）は、チェコ共和国Brno（ブルノ）に本社を置くベンダで、2007年6月に設立されました。大学のスピンオフとしてスタートし、CESNET（チェコ共和国の学術ネットワークの運用機関）内で検証された次世代ネットワークのモニタリングとセキュリティのノウハウを、現在は商用ビジネスとしてグローバルに展開しています。

Flowmon社は、この分野で最も成長の早い企業の一つとなっており、関連ソリューションは現在全世界で600社以上の導入実績があります。日本国内ではオリゾンシステムズ株式会社が2012年から国内販売総代理店としてFlowmon製品の取り扱いを開始し、大規模ネットワークユーザを中心として業種／業界を問わず、130社以上の導入企業実績があります。

詳細については、https://www.orizon.co.jp/products/flowmon を参照してください。

A10 Networks / A10ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションを提供することを使命としています。

詳しくはホームページをご覧ください。
www.a10networks.co.jp
Facebook：http://www.facebook.com/A10networksjapan

A10ネットワークス株式会社

www.a10networks.co.jp
a10networks.co.jp/contact

お問い合わせ：

Part Number: A10-SB-19129-JA-01 Apr 2018