データセンターのDDoS防御

コロケーションおよびデータセンタープロバイダー向け
高パフォーマンスで多機能なDDoS攻撃対策

課題：

DDoS攻撃は連鎖的に被害を及ぼすため、データセンターの1つのテナントが攻撃されれば、すべてのテナントにリスクが及びます。DDoSは現在、データセンターのダウンタイム発生原因の第3位ですが、さらに増加を続けているため、その防御はこれまで以上に重要です。

ソリューション：

A10 Thunder TPSは、高パフォーマンス・多機能で高度な設定が可能なDDoS防御ソリューションを実現します。自動化された脅威の検出と防御機能、詳細なサービス保護ポリシーが提供されます。

利点：

- ハードウェアベースの高速処理によりマルチベクトル型DDoS攻撃から効果的に保護
- 的確なトラフィックのベースライニングに基づき脅威の検出と防御を自動化
- 優れた拡張性と柔軟な設定による高度な攻撃の検査と防御
- 柔軟な導入 - オープンスタンダードとRESTful aXAPIに対応したカスタムのシステムとの容易な統合

企業は予測可能な運用、自社での運用より優れたROI、より強固なセキュリティを求めてプロバイダーの提供するデータセンターを利用します。企業の最も価値ある資産を扱うデータセンターにとって、完全性の維持とサービス中断の防止は最も重要な課題です。

Ponemon Instituteの最新のレポートによると、データセンターのダウンタイムの主な原因は、UPSシステムの障害、人為的ミス、DDoS（分散型サービス拒否）攻撃、天候、環境制御、発電機の故障およびIT機器の障害です。DDoS攻撃は2年前にはリストの最後に位置していましたが、その後急増して現在では第3位となり、ダウンタイムが5件発生するとそのうち1件がDDoS攻撃によって引き起こされています。

容易に実行できる上、低コストで大きな打撃を与えられることから、あらゆる業種でDDoS攻撃の被害が増加しています。リソースを共有するマルチテナント環境では個々のテナントのリスクが集約され、全体に影響するため、データセンターは格好の標的になっています。DDoS攻撃は標的の顧客だけでなく、データセンターはもちろん、他のテナントにも巻き添え被害を及ぼします。

ダウンタイムは収益の損失と顧客の不満足の原因になり、それによって顧客離れが進み、運用コストが上昇するだけでなく、新規顧客の開拓と維持に必要なマーケティングコストも増加します。しかし、最も深刻なのは、データセンターのブランドと評判を損なうことです。

また、ダウンタイムによって顧客にかかるコストも大幅に上昇します。Ponemonの概算ではDDoSによる中断を抑制するには平均82万2,000ドルかかりますが、これは、IT機器の障害復旧にかかる95万9,000ドルに次いで第2位です。

データセンターとそのテナントのデータのコスト増加を防ぐには、データセンターのサービスのすべてのレベルでセキュリティの課題に取り組む必要あります。多くのデータセンターはウイルスとマルウェアには高度なデータセキュリティと保護対策を用意していますが、大半はDDoS防御が不十分で、破滅的な結果を引き起こす可能性を見過ごしています。

課題

DDoS攻撃はネットワーク帯域幅、サーバーソケット、Webサーバースレッドと CPU使用率に影響を与えるボリューム攻撃とアプリケーションレイヤー攻撃を組み合わせ、ますます巧妙になっています。ボリューム攻撃はデータセンターの一次通信事業者の接続を飽和状態にし、その事業者がホストするアプリケーションとサービスへのアクセスを不能にします。アプリケーション攻撃は特定のホストを標的にし、アプリケーションリソースを過負荷状態にするため、本質的に区別されます。

DDoS攻撃は簡単かつ低コストで実行できるようになっただけでなく、量、速度、期間、複雑さのすべての面で増大しています。インターネットサービスプロバイダー（ISP）はボリューム攻撃防御の第一線になるべきですが、あてになりません。また、ファイアウォール、侵入防止システム（IPS）、ロードバランサーはネットワークの完全性を確保するには効果的なツールである反面、ステート枯渇攻撃には脆弱で、多くの場合、レイヤー7への攻撃の検出と防御には不十分です。データセンターを保護するために、データセンター事業者はそのネットワークインフラストラクチャーを標的にしたボリューム攻撃とアプリケーションレイヤー攻撃に対抗し、防御するための専用のDDoS対策ソリューションを導入する必要があります。

驚いたことに、ファイアウォール、SSL 証明書、ウイルス対策、VPN、アラート以外のセキュリティサービスを顧客に提供しているデータセンターはごく少数です。専用の DDoS 対策ソリューションを採用することによって、最新の管理された DDoS 防御サービスをテナントに提供できるため、他社との差別化を図り収益を増やすことができます。

A10 Networks Thunder TPS によるソリューション

拡張可能な高パフォーマンスのソリューションをデータセンターのエッジに導入することで、ダウンタイムを回避して、顧客の低速な下り回線接続とサーバーを保護することが可能です。

DDoS 攻撃は顧客に莫大な顧客コストを発生させ、顧客離れを促し、ブランドと評判を損ないます。A10 Networks® Thunder TPS™（Threat Protection System）製品ラインは優れたパフォーマンスによって、DDoS 攻撃からネットワーク全体を保護します。また、多様なボリューム攻撃や高度なアプリケーション攻撃に対抗してサービス可用性を確保できます。

Thunder TPS は帯域幅、1 秒あたりのパケット処理量、1 秒あたりの接続量、およびブラック / ホワイトリストで最高のパフォーマンスを提供するよう設計されているため、毎日のように発生する DDoS 攻撃やその他セキュリティの異常を、余裕をもって処理可能です。

ネットワーク構成やポリシーは企業によって異なるため、Thunder TPS の導入と統合にはさまざまなオプションが用意されています。aXAPI® REST ベース API を介して、サードパーティの分析システムでは必要に応じてトラフィックを指定して、クリーニングのために転送できます。同様に、オーケストレーションソリューションを使用して、データセンターの Thunder TPS システムに特定のエンドユーザー専用のポリシーを提供できます。

A10 Networks aGalaxy® 集中管理システムでは、複数の Thunder TPS デバイスの管理を一元化するため、運用効率が向上し、コストを削減できます。すべての管理タスクは 1 つの場所に統合されるため、管理者はすべてのデバイスに一貫性のあるポリシーを容易に適用できます。

また、aGalaxy の Web ユーザーインターフェイスを使用して仮想サーバー、Thunder TPS 管理、TPS 保護対象オブジェクトのステータスを表示できます。

ネットワークのキャパシティを超えるボリューム攻撃は、Verisign の DDoS 防御サービスで処理できます。Verisign は DDoS 保護サービスを強化するため、世界 75 か所の拠点と 2Tbps を超えるグローバルなキャパシティを駆使しています。

大手データセンターではサービス可用性を維持するために A10 Thunder TPS を導入し、マネージド DDoS セキュリティソリューションを顧客に提供して収益を増やしています。

機能と利点

Thunder TPS の機能と利点は以下のとおりです。

- **インフラストラクチャーに対する一般的な攻撃をハードウェアベースで防御：** Thunder TPS では、ハードウェアに対する 60 個の一般的な攻撃を検出および防御できるため、その非常に強力な CPU をより複雑なアプリケーションレイヤー攻撃の検出と防御に使用できます。
- **脅威の高度な検出と防御：** システムが多様なマルチプロトコルのカウンターと動作インジケーターにアクセスして正常なネットワークの状態を学習するため、異常を正確に検出できます。また、正当なトラフィックのドロップを最小化するため、動的な防御ポリシーによって疑わしいトラフィックには段階的に厳格化される対策が適用されます。DevOps ではイベントによってトリガーされるスクリプトを活用して、運用の機敏性を向上させることができます。
- **詳細なトラフィックレートの適用：** Thunder TPS は独自の機能により外部接続ごとのトラフィックレートを追跡できます。これらのトラフィックパターンは予測可能で、異常を簡単に特定・防御できるため、他の顧客に影響することはありません。

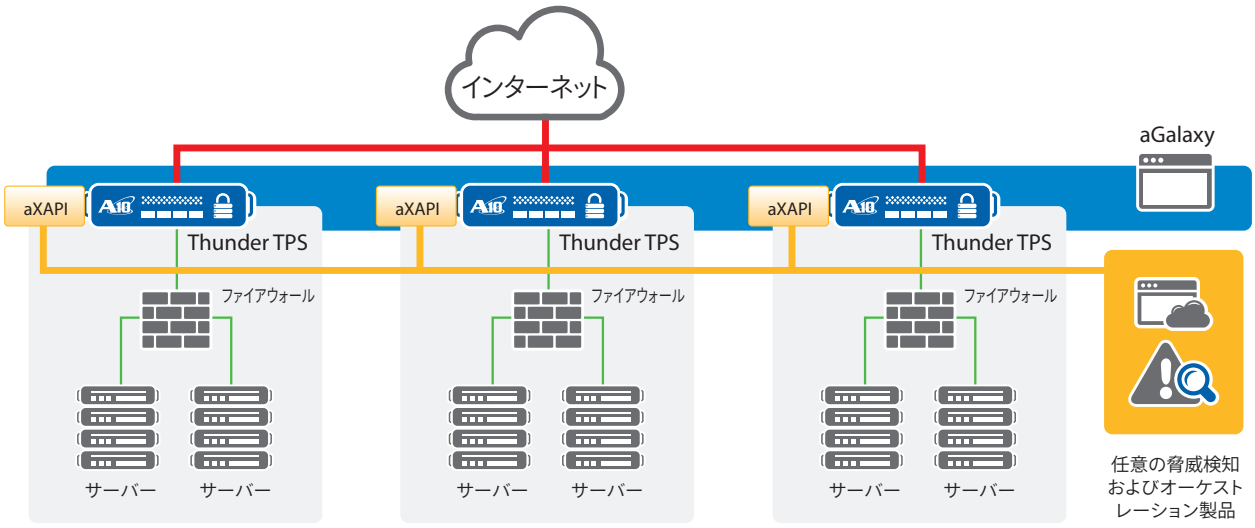

図 1：複数のデータセンターを保護する Thunder TPS とそれを制御する aGalaxy。
サードパーティ製脅威検知およびオーケストレーションソリューションでは aXAPI を使用した完全な制御や選択的なポリシーの適用が可能

- **プログラム可能なポリシーエンジン：**Thunder TPSではシステムの状態と統計情報へのアクセスに加え、高度なアプリケーションとセキュリティのポリシーを容易に施行できます。パターンマッチングのツールには、正規表現（regex）とBerkeley Packet Filter（BPF）が使用されています。
- **ThreatSTOPの提供するA10 Threat Intelligence Service：**このサービスは、DShieldやShadowserverを含む30以上の脅威情報ソースが提供するレピュテーションデータを統合して強化されているため、既知の悪質なソースとの間を往来するトラフィックはThunder TPSによって即座に認識されブロックされます。A10 Threat Intelligence Serviceには以下の利点があります。

  ー 新しい脅威からのネットワークの保護

  ー スパムやフィッシングなど、DDoS以外の脅威の防止

  ー Thunder TPSの防御効率向上

  脅威情報ネットワークによってインターネット上の潜在的な侵入者が継続的に表示されるため、そのグローバルな情報を活用して悪質なインターネットサイトからのトラフィックをブロックするとともに、Thunder TPSで既知のボットや攻撃元を特定する必要がなくなり、その分の負荷が軽減されます。
- **プログラム可能な統合：**高度に複雑化するネットワークには、緊密な統合が必要です。多くのカスタムシステムを使用していても、Thunder TPSならネットワークプロトコルのオープンな標準とaXAPI APIを活用して簡単に統合できます。
- **IPv6への対応：**急増するIPv6の採用に対応しており、データセンタープロバイダーのセキュリティインフラストラクチャーはIPv4経由とIPv6経由の両方の攻撃に対処できます。

まとめ ー 高パフォーマンスで多機能なデータセンター事業者向けDDoS防御ソリューション

A10は被害の連鎖をもたらす攻撃から設備を保護し、完全性を維持する必要のあるデータセンター事業者に向けて、拡張性と構成の柔軟性に優れたDDoS防御ソリューションを提供しています。脅威防御システムThunder TPS製品ラインでは包括的なツールによって迅速なトラフィック分析が可能になり、サービスの中断を最小化することができます。

次のステップ

A10ネットワークスの製品とソリューションの詳細については、A10の営業窓口にお問い合わせいただくか、www.a10networks.co.jp をご覧ください。

A10 Networks / A10ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はアプリケーションネットワーキング分野におけるリーダーとして、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、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ご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
〒105-0001
東京都港区虎ノ門4-3-20
神谷町MTビル16階
TEL：03-5777-1995
FAX: 03-5777-1997
jinfo@a10networks.com
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
anz_sales@a10networks.com

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト**www.a10networks.co.jp**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-SB-19140-JA-02
Mar 2016