DMZのセキュリティの拡張と最適化

DMZにおけるセキュリティ機能の最適化

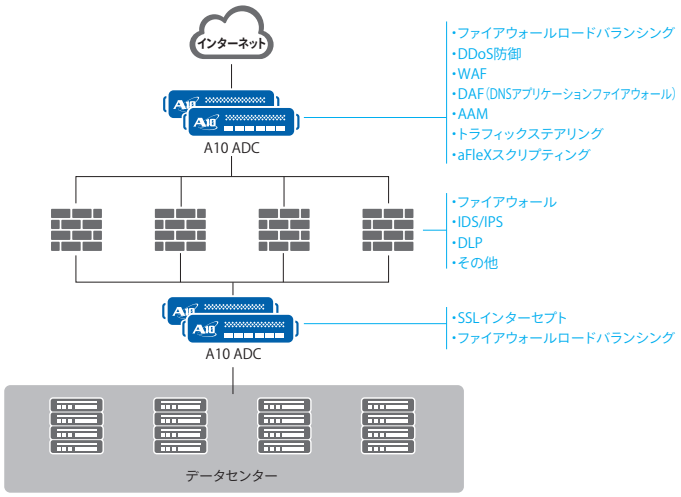
重要なアプリケーションの保護

セキュリティの専門家は、ますます巧妙になるサイバー攻撃に対するセキュリティをアプリケーションに強制しつつ、正規のエンドユーザーに十分なアクセスを提供するという困難な道を歩んでいます。セキュリティを厳しくしすぎるとエンドユーザーがアプリケーションを使用しにくくなり、セキュリティを緩めすぎると組織が攻撃を受けて収益を失ったり、ブランドが損害を受ける可能性があります。ほとんどすべての組織には、誰もがアクセスできるようにする必要があるアプリケーションがあります。技術の急速な進化に伴い、組織は十分なセキュリティの提供と、正規ユーザーに対するアクセス保証との間で、デリケートなバランスをとるという課題に直面しています。

- **セキュリティデバイスの拡張と暗号化通信** – ネットワークの成長につれて、既存のセキュリティインフラストラクチャーを拡張する必要が生じます。ネットワークのキャパシティを増やす場合には、高パフォーマンスのセキュリティデバイス（ファイアウォールなど）への切り替えを考慮する必要がありますが、それはコストがかかる複雑な作業です。暗号化通信（HTTPS、SSHなど）によってコンテンツを保護すると、これらのDMZセキュリティデバイスに過大な負荷がかかります。詳細なパケット検査でアプリケーショントラフィックの分析に、多くのリソースを使用する暗号化/復号化機能が実装されるからです。未知の公開サイトへのトラフィックを復号化して検査しないと、情報漏えいやマルウェア（APT攻撃を含む）に対して無防備な盲点ができてしまいます。

- **帯域幅消費型DDoS攻撃の登場** – 新種のセキュリティ脅威により、セキュリティスタッフは新たな課題に直面していますが、そのなかで最も目立つのは、Webサイトや重要なネットワークインフラストラクチャーに対するDDoS（分散型サービス拒否）攻撃の増加です。DDoS攻撃は標的型のWeb攻撃とは異なり、公開されたインフラストラクチャーを大量のネットワーク攻撃でオーバーフローさせる攻撃であり、アプリケーションに対する攻撃を検知しにくく、正規のユーザーがネットワークサーバーやアプリケーションサーバーを利用できなくなります。組織内外のユーザーにサービスを提供しているネットワークインフラストラクチャーおよびアプリケーションがDDoS攻撃によって使用不能になると、この問題はさらに悪化します。リソースが使用不能になると、顧客満足度が低下し、ブランドのイメージが損なわれ、収益が低下しますが、それだけでなく、DDoS攻撃は他の悪事（銀行口座からの窃盗など）が行われている間ITスタッフの注意をそらすためにも利用されます[1]。

- **セキュリティサービスの静的な適用** – 従来のネットワークセキュリティサービスは、特定のサービスまたはユーザーグループ専用の特定のVLANまたはサブネット上でインラインで適用する必要がありました。このことは残念ながら、すべての負荷を常時処理するためには、個々のフローに実際に必要なサービスの種類にかかわらず、高価なネットワークセキュリティ機器を過剰にプロビジョニングする必要があることを意味します。予算とリソースには限りがあるため、より柔軟で最適化されたアプローチを使用して、必要なときにだけサービスチェイニングを動的に適用するのが理想的です。



DMZセキュリティデバイスの拡張、オフロード、および高速化

DMZセキュリティインフラストラクチャーの拡張と最適化

A10ネットワークスは、新しいプレミアム機種のThunder™シリーズおよび既存のAXシリーズのアプリケーションデリバリーコントローラー（ADC）と、Thunder TPS（Threat Protection System）を提供しています。これらはすべてA10独自のACOS（Advanced Core Operating System）をベースに構築されており、豊富なセキュリティの機能セットを備えています。これらのA10製品により、DMZセキュリティインフラストラクチャーの効率を大幅に向上し、セキュリティの強化役立ちます。

セキュリティデバイスの拡張と暗号化通信は、ネットワークが成長してその複雑さと規模が増すにつれて重要な要件となります。

- A10 Thunder ADCのファイアウォールロードバランシング（FWLB）は、HAを容易に実現し、既存のネットワークファイアウォールのパフォーマンスを最大化します。ファイアウォールは通常、アクティブ/パッシブ構成でHAをサポートしますが、この構成はパフォーマンスの向上が必要になった場合アップグレード費用がかかります。FWLBは、必要に応じて追加のファイアウォールを付け加えることでDMZセキュリティ機器を拡張するので、既存のデバイスを完全に置き換える必要がありません。また、パフォーマンスの制約があるセキュリティデバイスから、多くのリソースを使用し負荷のかかる処理を取り去ります（SSLオフロード、DDoS防御、許可リスト、拒否リストなど）。FWLBは、使用可能なファイアウォールの間で負荷を分散することにより、ファイアウォールの保守を簡単にし、ネットワークの中断を最小限に抑えます。その結果、回復力に富み適応性の高いファイアウォール運用を実現できます。

[1] http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/

- HTTPSに使用されるTLS/SSL暗号化は、内部サーバーから組織のファイアウォールの外にいるユーザーへインターネットを介して送られる機密データを守るための、最も一般的なセキュアネットワーク通信方式です。SSLのハンドシェイクとバルク暗号化の処理はCPUを集中的に使用するタスクなので、ファイアウォール、侵入防止システム（IPS）、およびアプリケーションのコンテンツを平文で処理する必要があるその他のDMZセキュリティデバイスのパフォーマンスに影響を与えます。リバースプロキシーとして動作するSSLオフロード機能により、Thunder ADCはこれらのセキュリティアプライアンスをSSLトランザクションの負荷から解放し、より付加価値の高い分析やセキュリティ機能にコンピューティングリソースを割り当てられるようにします。SSLオフロードは、DMZセキュリティインフラストラクチャーを最適化し、暗号化されたトラフィックの負荷の増大に応じた拡張が可能です。

- **SSLインターセプト機能**は、DMZを介してインターネットへ向かうユーザートラフィックを復号化することで、エンタープライズのセキュリティ防御の盲点を排除するフォワードプロキシーです。SSLインターセプトはSSLオフロードと同様に、アウトバウンドトラフィックに対してセキュリティポリシーを適用するために、トラフィックをDMZセキュリティデバイスに転送する前に復号化して検査します（ファイアウォール、IDS/IDP、DLPなど）。データはその後再び暗号化され、最終的な外部の宛先へ向けて送信されます。A10 ADCプラットフォームの専用SSLセキュリティプロセッサーは、CPUを集中的に使用するSSL暗号化機能の負荷を軽減し、セキュリティデバイスを本来の検査機能や防御機能に活用できるようにします。

新たなDDoS攻撃の規模、頻度、および帯域幅消費量は増加を続けており、問題が深刻化しています。これらの攻撃は、正規のプロトコルを使用するボットネットの大規模な分散ネットワークを活用してネットワークおよびサーバーリソースを過負荷状態にし、従来のシグネチャーベースのセキュリティデバイスを回避します。また、DDoS攻撃ではギガビット/秒単位で測定される膨大な量のデータが送りつけられるため、比較的パフォーマンスが低いほとんどのセキュリティデバイスは圧倒されてしまう可能性があります。その結果、DMZにおいて、より新しく高パフォーマンスなDDoS防御ソリューションが必要とされるようになっています。

- DMZセキュリティアプライアンスをさらに防御し、このような帯域幅消費型攻撃による負荷を軽減するために、A10のADC製品ラインにはDDoS検知/緩和ソリューションが含まれています。ADC製品とTPS製品は、スローHTTP攻撃（Slowlorisなど）、大量のTCP SYNフラッド、異常なプロトコルの使用のようにネットワークレイヤーとアプリケーションレイヤーの両方を含む多面的な（マルチベクター）攻撃に対する防御として、DDoSセキュリティ機能を提供しています。

動的なセキュリティチェインの選択的適用により、各アプリケーションまたはユーザーグループがそれぞれ適切なセキュリティポリシーを選択的に受け取るようにすると同時に、DMZセキュリティインフラストラクチャーをインラインで全パケットを処理する負荷から解放することができます。

- **トラフィックステアリングおよびサービスチェイニング**技術は、プロトコルやコンテンツなど特定の属性に基づいたフローのリダイレクトを可能にします。A10のADCアプライアンスは、最適化またはセキュリティ処理のために、タイプ別のトラフィックをその「フィンガープリント」に基づいて適切なサービスへリダイレクトすることができます。これにより、ある特定のセキュリティデバイスによる処理が必要なトラフィックだけがそのデバイスに送られるようにするサービスチェイニングポリシーが実施されます。結果、ネットワークの効率が向上し、リソースの制約があるセキュリティデバイスへの投資が拡張され最適化されます。オープンAPI（aXAPI®）とICAPがサポートされているため、トラフィック管理コントローラーとの連携やリダイレクトポリシーの動的なアップデートが可能です。

まとめ

A10の製品は、セキュリティとDMZ環境に関する課題を解決しアプリケーションの高可用性、スピード、およびセキュリティを確保するために、さまざまなソリューションを提供します。

A10 Thunder製品は現在多くの組織で採用されていますが、それにはいくつもの理由があります。その理由には、高度な機能を含むすべての機能を追加ライセンスの購入なしで使用可能なライセンス体系や、フォームファクターの柔軟な選択肢が用意され特定のネットワークニーズをサポートできるよことなどが含まれます。

A10 Networksについて

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であるA10 Networksは、ネットワーキングと、セキュリティ分野における革新的なソリューションの提供を目指して2004年に設立されました。あらゆるお客様のアプリケーションを高速化、最適化するとともに、そのセキュリティの確保をも支援することができる高性能な製品群を開発しています。当社は米国シリコンバレーに本拠地を置き、米国各地のほか世界各国に拠点を置いています。詳しくはホームページをご覧ください。
www.a10networks.com

A10ネットワークス株式会社について

A10ネットワークス株式会社は、米国A10 Networksの日本法人として、2009年3月に設立されました。米国に本社をもつ「日本企業」として、日本のお客様の意見や要望を積極的に製品に取り入れると共に、ネットワーキング・セキュリティ分野のテクノロジリーダーとして、常に革新的なソリューションをタイムリーに且つリーズナブルな価格で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
brazil@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: 19101-JA-03 Feb 2014