DNSアプリケーションファイアウォール

Thunder ADCによるDNSインフラストラクチャー保護とパフォーマンス最適化

課題:

攻撃者はDNSインフラストラクチャーを標的に、サービスを妨害したり、DNSサーバーを強力なDDoS攻撃の踏み台として悪用

解決策:

A10 Thunder ADCは、強力かつ包括的なDNSアプリケーションファイアウォールによってDNSインフラストラクチャーを攻撃から保護

メリット:

- DNSサーバーを標的にしたDDoS攻撃を防御
- 無効なトラフィックを削除したりDNS応答をキャッシュに保存することで、DNSサーバーへの負荷を最大70%軽減
- ロードバランシングと高可用性によりアップタイムを最大化
- ラックマウント可能な1台のアプライアンスで毎秒2500万件のDNSクエリーを処理する拡張性を実現

インターネット通信のほぼすべての機能は、Webサイトの閲覧から電子メールの送信やファイル転送にいたるまで、DNSサーバーによるドメイン名解決を必要とします。攻撃者によってサービスプロバイダーのDNSサーバーへのアクセスが遮断されると、そのサービスプロバイダーの加入者はインターネットへのアクセスやVoIP通話などを行うことが実質的にできなくなります。同様に、企業のDNSインフラストラクチャーが正常に機能しなくなった場合は、インターネットユーザーはその企業のWebサーバーやメールサーバーなどの重要なサーバーにアクセスできなくなります。

サイバー犯罪者や政治的ハッカーは、ユーザーを通信不能にする方法だけでなく、DNSサーバーを他の目的に悪用する方法も知っています。たとえばこれらの攻撃者は、DNSサーバーのキャッシュを改ざんして正規ユーザーを不正なサイトに誘導できます。さらに、DNSサーバーを悪用して分散サービス拒否（DDoS）攻撃の規模を拡大することもできます。DNSアンプ攻撃はDDoS攻撃の規模を最大54倍[1]に拡大できるため、攻撃者が大規模なDDoS攻撃を実行するための簡単な手段となります。近年の大規模なDDoS攻撃の多くはアンプ攻撃でした。

A10ネットワークスのThunder® ADC（アプリケーションデリバリーコントローラー）製品ラインは、あらゆる種類のDNSの脅威からの包括的で強力な防御を可能にします。Thunder ADCは、処理負荷の大きいネットワーキングタスクを処理できるように設計されています。Advanced Core Operating System（ACOS®）をベースにしたThunder ADCは、共有メモリーアーキテクチャーとFlexible Traffic Accelerator（FTA）を活用して極めて高いパフォーマンスを実現します。

Thunder ADCのDNSアプリケーションファイアウォールの機能は次のとおりです。

- 直接のDNS攻撃や脆弱性攻撃からインフラストラクチャーを保護して、企業の信用低下や訴訟リスクを回避します。
- 不正なソースからの要求をブロックして、インフラストラクチャーが第三者に対する攻撃の踏み台にされることを防止します。
- ロードバランシングとキャッシングによってDNSのパフォーマンスと可用性を最適化します。
- A10の高性能なACOSオペレーティングシステムによって大規模なDDoS攻撃に耐えます。
- プロトコル検証によってDNSサーバーの負荷を最大70%軽減します。
- 業界標準のDNSセキュリティ拡張機能（DNSSEC）のパススルーサポートを実現します。

課題

高まるDNSセキュリティ脅威

DNSサーバーが不名誉にも主要な攻撃ターゲットとなったことには2つの理由があります。1つ目は、攻撃者にとってDNSサーバーをオフラインにすることは、多数のインターネットユーザーをインターネットにアクセス不能にするための簡単な手段であるからです。攻撃者がサービスプロバイダーのDNSサーバーを応答不能にした場合、そのサービスプロバイダーの加入者はドメイン名の解決、Webサイトへのアクセス、電子メールの送信といった重要なインターネットサービスを利用できなくなります。DNS攻撃はこれまでにも、多くのサービスプロバイダーのDNSサービスを何時間あるいは何日にもわたってダウンさせたことがあり、極端なケースでは、加入者による集団訴訟を引き起こしたこともあります。攻撃者によってDNSインフラストラクチャーへのアクセスが遮断されて、ユーザーが重要なサービスを利用できなくなった場合は、企業の収益が減少したりブランドが損なわれたりする可能性があります。

[1] UDPベースのアンプ攻撃：https://www.us-cert.gov/ncas/alerts/TA14-017A

さらに、攻撃者はDNSサーバーを利用してDDoS攻撃を増幅させることができます。DNSリフレクション攻撃の場合は、攻撃者は実際の攻撃ターゲットのIPアドレスをスプーフィング（偽装）します。攻撃者が送信するクエリーの指示に従って、DNSサーバーは多数のDNSサーバーに反復的にクエリーを送信したり、大量の応答を攻撃ターゲットに送信したりします。その結果、多数の強力なDNSサーバーから送信されてくるDNSトラフィックによって、攻撃ターゲットのネットワークが飽和状態になります。

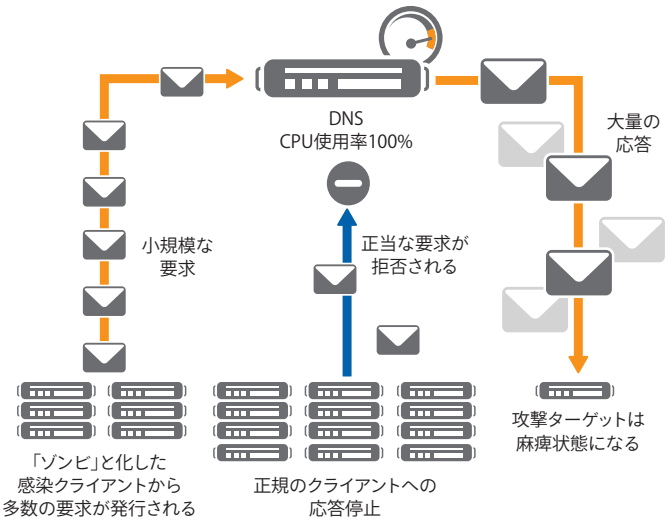

図1：DNSアンプ攻撃

DNSサーバーが攻撃の最終ターゲットでない場合でも、DNSリフレクション攻撃の結果としてDNSサーバーのダウンタイムや障害が発生する可能性があります。DNSはすべてのDDoS攻撃の8.95%を占めているため[2]、DNSサーバーをホストしている組織は自身のDNSインフラストラクチャーを保護する必要があります。

A10ネットワークスのThunder ADCソリューション

DNSサーバーは、直接の攻撃ターゲットになったり、アンプ攻撃の踏み台になったり、不正な形式の要求を送りつけられたりという形で、攻撃を受けます。ほとんどの組織では、DNSサーバーを監視したり最先端の攻撃からDNSサーバーを保護したりするために必要なレベルのセキュリティ対策が導入されていないため、DNSインフラストラクチャーは攻撃に対して無防備なままになっています。

DNSサーバーを保護するためには、多数の脅威を抑制できるとともに、卓越したアプリケーションパフォーマンスを実現できるDNSアプリケーションファイアウォール（DAF）を導入する必要があります。それを実現するのがA10 Thunder ADCです。Thunder ADCは、共有メモリーアーキテクチャーと64ビットの拡張性を活用して高速で強力な保護を実現します。

Thunder ADCの一部として、A10ネットワークスは強力な統合型DNSアプリケーションファイアウォールを提供しています。DNSアプリケーションファイアウォールは、バッファーオーバーフロー、不正な形式の要求、およびサービス拒否（DoS）攻撃を防止して、DNSサーバーを攻撃から保護します。さらに、Thunder ADCは複数のDNSサーバーをロードバランシングすることや、DNS応答をキャッシングすることもできるため、DNSサーバーが大きな負荷や大規模な攻撃に対処することを可能にする拡張性も提供します。

機能と利点

Thunder ADCのDNSアプリケーションファイアウォールにより、組織では以下のことが可能になります。

- **重要なDNSサーバーを直接攻撃や脆弱性攻撃から保護**
  DNSアプリケーションファイアウォールは不正な形式のDNS要求をブロックして、DNSインフラストラクチャーをバッファーオーバーフローやDoSから保護します。さらに、IPベースの接続レート制限と同時接続制御によってDDoS攻撃を抑制します。ポリシーベースのサーバーロードバランシング（PBSLB）によって、A10は既知の不正なソースからの要求をブロックできます。お客様は、最大800万件のIPアドレスのリストをインポートして、ユーザーをブラックリストに登録したり、既知の信頼できるソースのみにアクセスを許可することが可能です。

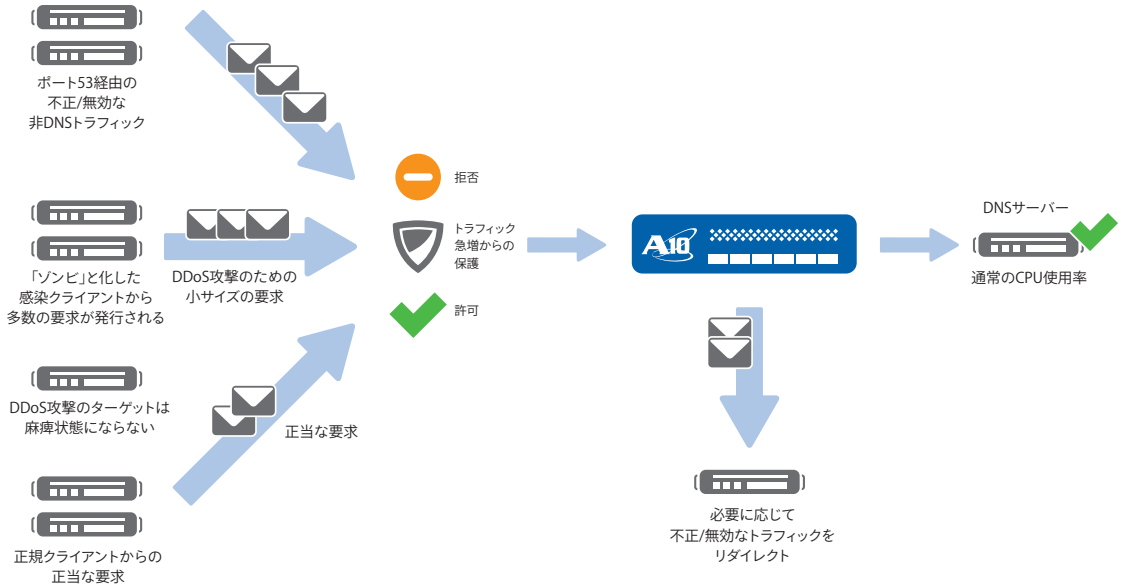

図2：組み込み型のDNSアプリケーションファイアウォールによって、
Thunder ADCは既知の不正なクライアントからの攻撃、非DNSトラフィック、およびDNSクエリーを検知可能

[2] Prolexic Global DDoS Attack Report（2014年）

- **DNSアンプ攻撃を阻止し評判低下や信用失墜を回避**
  – 攻撃者はDNSサーバーを悪用してDDoS攻撃を増幅するため、組織は自身のサーバーが他組織に対する攻撃の踏み台にされることを防止する必要があります。A10のDNSアプリケーションファイアウォールは接続レート制限をサポートしているだけでなく、ソースIPアドレスに基づいてトラフィックを制限できます。

- **高度なスクリプティングによってDNS構成の不具合を「仮想的に修復」**
  – A10ネットワークスのaFleX®ディープパケットインスペクション（DPI）スクリプティングテクノロジーのポリシーは、DNSクエリーとDNS応答を変換して、DNS再帰のような特定タイプの攻撃を防止できます。さらに、特定タイプのDNSクエリーを強制的にTCPに戻すようにaFleXのルールを記述して、従来よりコネクションの少ないUDPトラフィックのIPスプーフィング攻撃を防止できます。

- **DNS攻撃を上回るレベルにDNSインフラストラクチャーを拡張**
  – 高度なサーバーロードバランシングを利用することで、複数のDNSサーバーを導入して可用性を最大化できるとともに、大規模な攻撃に耐え得るようにキャパシティを拡大できます。A10の強力なACOSプラットフォームと高速な共有メモリーアーキテクチャーは超高速なパフォーマンスを実現します。

- **キャッシングとプロトコル検証によりDNSサーバーの負荷を最大70%軽減**
  – DNSサーバーは非DNSトラフィックによって攻撃を受けることがよくあります。Thunder ADCは、プロトコルのチェックと適用を通じてDNSトラフィックを正しく識別してルーティングすることで、DNS以外のトラフィックがDNSインフラストラクチャーに侵入することを防止します。キャッシングは、DNSサーバーを攻撃から保護するだけでなく、必要なDNSサーバーの数を減らすことで設備コストを削減します。

- **DNSSECセキュリティ拡張機能を適用してDNSデータを検証**
  – Thunder ADCのDNSアプリケーションファイアウォールは、検証済みのDNSSECパススルーサポートを通じて、組織がDNSキャッシュのポイズニングやスプーフィングのような脅威を防止することを可能にします。DNSアプリケーションファイアウォールは、VeriSign DNSSEC相互運用性ラボでのテストに合格しているため、業界標準のDNSセキュリティ拡張機能をサポートすることが保証されます。DNSアプリケーションファイアウォールはTCP経由で送信されたDNSクエリーを認証したり、必要に応じてUDP応答をTCPにリダイレクトしたりすることで、ソースが正当なものであることを確認して、スプーフィングなどの脅威を防止することもできます。

- **パフォーマンスをリニアに拡張してキャパシティを最大化**
  – Thunder ADCのDNSアプリケーションファイアウォールは共有メモリーアーキテクチャーをサポートしているため、マルチコアプロセッサーを最大限に活用できます。Thunder ADCの共有メモリーアーキテクチャーはパフォーマンスを向上させるだけでなく、プロセッサーコアが全接続数をリアルタイムで完全に把握できるため、レートリミットの精度も高めます。

- **IPv4とIPv6のDNSトラフィックを保護**
  – Thunder ADCのDNSアプリケーションファイアウォールは、IPv4とIPv6の両方の通信プロトコルについて同じレベルの保護を実現します。Thunder ADCはIPv6移行技術をサポートしているため、使用されているIPバージョンにかかわらず、組織はDNS要求を簡単に処理できます。DNSアプリケーションファイアウォールが統合されたThunder ADCは、DNS脅威からの業界最高レベルの包括的な保護を可能にする一方で、DNSアプリケーションのパフォーマンスを向上させることができます。

DNSアプリケーションファイアウォールの機能

DNS DDoS攻撃の防御とDNSサーバーの負荷軽減

- 接続レート制限
- ソースIPベースの接続レート制限
- 最大800万件のIPアドレスと1万件のサブネットが登録されたブラックリストとホワイトリストを使用したポリシーベースのサーバーロードバランシング（PBSLB）
- DNS認証
- 脆弱性攻撃を防止するaFleXポリシー
- 特定名のドメイン名に基づいたトラフィック制限
- 最大クエリー長保護・DNSキャッシング
- DNSトラフィックのロードバランシング

Thunder ADCによって防御可能なDNS DDoS攻撃

- DNS ANY攻撃
- 不正な形式のDNSクエリー
- DNSアンプ攻撃
- レイヤー3に対する帯域幅消費型DDoS攻撃 – SYNフラッド、ICMPフラッド、UPDフラッド、Ping of Death、Smurf攻撃、LAND攻撃、フラグメントパケット

まとめ – A10のDNSアプリケーションファイアウォールによるDNSインフラストラクチャーの保護

データセンターのセキュリティ脅威が高まる中で、組織はDNSインフラストラクチャーを攻撃から保護できるソリューションを必要としています。セキュリティソリューションはそれらの進化に適応して、トラフィックの急増に対応してビジネスを常に円滑に運営するための処理能力を提供する必要があります。

A10のソリューションにより、組織はDNSサーバーの保護が可能です。Thunder ADCのDNSアプリケーションファイアウォールは、DDoS攻撃、DNSキャッシュポイズニング、およびカスタム脆弱性攻撃に対する強力な防御を可能にします。Thunder ADCは、統合型のロードバランシング、プロトコル検証、およびDNSキャッシングによって、DNSインフラストラクチャーの総合キャパシティを拡大できます。A10 Thunder ADCは、世界中の数千の組織で導入されており、DNSサーバーの可用性向上、高速化、セキュリティ強化を実現します。

次のステップ

A10ネットワークスのアプリケーションデリバリーコントローラーThunder ADC製品ラインの詳細については、A10ネットワークスの担当者にお問い合わせください。

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ています。世界中で数千社にのぼる大企業やサービスプロバイダー、大規模Webプロバイダーといったお客様のデータセンターに導入され、アプリケーションとネットワークを高速化し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-19136-JA-01
June 2015