ソリューションブリーフ

DNSアプリケーションファイアウォール

A10 Thunder シリーズによる 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

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 A10 Thunder シリーズは、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。A10 Thunder シリーズは、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。

A10 Thunder シリーズの 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

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

ソリューション

A10 Thunder シリーズは、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

利点

- 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

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

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。

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。

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。

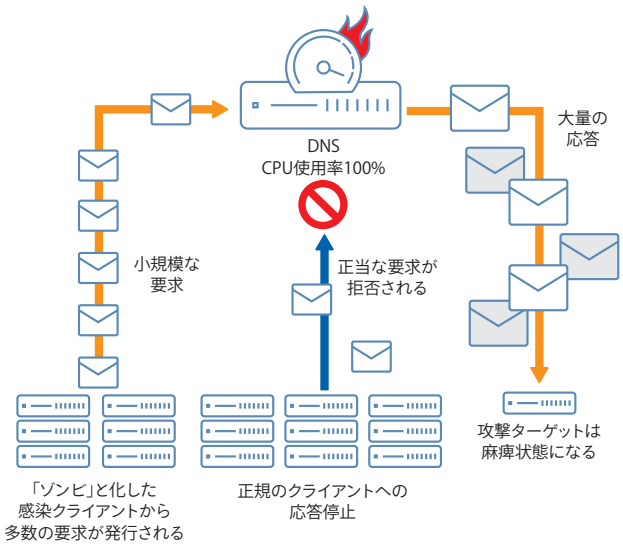

図1： DNSアンプ攻撃

A10ネットワークスの Thunderシリーズソリューション

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シリーズです。A10 Thunderシリーズは、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。

A10 Thunderシリーズの一部として、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、A10 Thunderシリーズは複数の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

A10 Thunderシリーズの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。
- **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

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

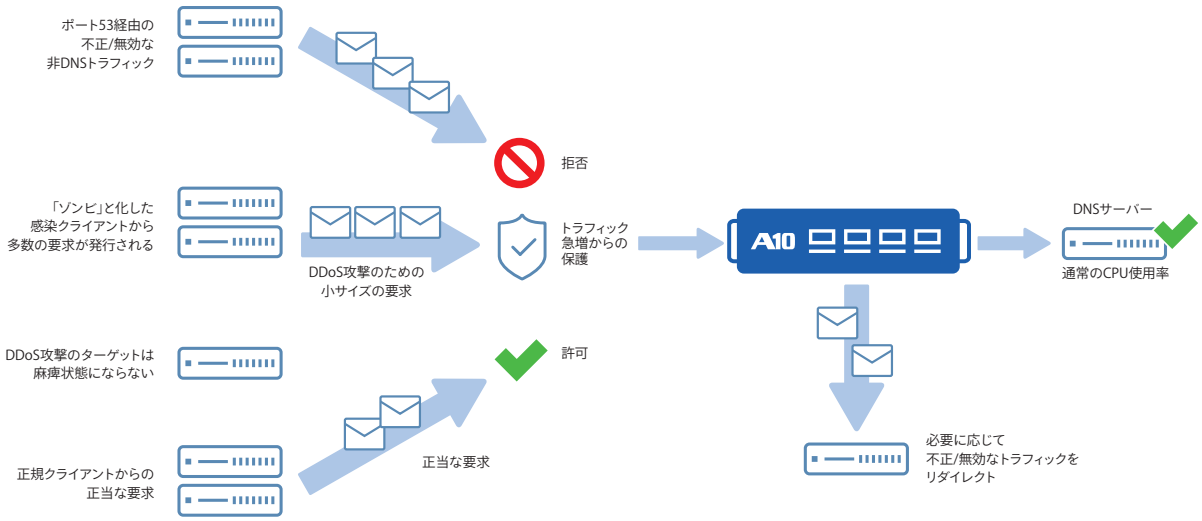

図2： 組み込み型のDNSアプリケーションファイアウォールによって、A10 Thunderシリーズは既知の不正なクライアントからの攻撃、非DNSトラフィック、およびDNSクエリーを検知可能

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。A10 Thunder シリーズは、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**
  A10 Thunder シリーズの 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**
  A10 Thunder シリーズの 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。A10 Thunder シリーズ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**
  A10 Thunder シリーズの 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。A10 Thunder シリーズは 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 A10 Thunder シリーズは、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

- 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

A10 Thunder シリーズによって防御可能な DNS DDoS 攻撃

DNS DDoS 攻撃の防御と DNS サーバーの負荷軽減

- 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。A10 Thunder シリーズの 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。A10 Thunder シリーズは、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 シリーズは、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 A10 Thunder シリーズの詳細については、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 は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 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社を置き、世界中のお客様にサービスを提供しています。

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。

- URL：https://www.a10networks.co.jp/
- X（旧 Twitter）：https://twitter.com/a10networksjp
- Facebook：https://www.facebook.com/A10networksjapan

Learn More

About A10 Networks

お問い合わせ

A10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

Part Number: A10-SB-19136-JA-02 JUN 2024