Always Secure. Always Available.

ソリューションブリーフ

ネットワークサービスの基幹となるDNSのセキュリティ強化

DNS over TLS/HTTPSやDNS RPZに対応したセキュアで可用性の高いDNSサービスの実現

DNSセキュリティの必要性

インターネットを通じたコミュニケーションは、宛先サーバーのドメイン名をIPアドレスに変換するDNS（Domain Name System）に大きく依存しています。近年利用が拡大しているクラウドサービスにおいても、サービスへのアクセスはドメイン名を通じて行われており、高速なネットワークアクセスを実現するためにWebサービスやクラウドサービスにおいて広く利用されているコンテンツ配信ネットワークのサービスもDNSに大きく依存しています。ひとたびDNSに障害が発生すると、インターネット上のWebサーバーなどへのアクセスは容易に阻害されてしまいます。現に、2016年にDNSサービスを提供する会社に大規模なDDoS攻撃が行われた際には、多くのWebサービスやクラウドサービスへのアクセスが出来なくなった事態が発生しました。また、アンプ攻撃と呼ばれるタイプのDDoS攻撃にオープンなDNSリゾルバが他のサービスに対する攻撃元として利用されたり、攻撃者がDNSのTXT応答に悪意のあるコードを埋め込んだりすることもあります。そのため、DNSには高い可用性とセキュリティが求められます。

DNSはインターネットの初期から利用されてきたこともあり、通信の秘匿性に関してこれまで不十分な面がありました。例えば、通信が暗号化されたHTTPSでWebサーバーにアクセスする場合においても、DNSへのWebサーバーの名前解決の問い合わせ（クエリ）と応答はデフォルトでは平文で通信され、通信を盗聴することでクライアントのアクセス先に関わる情報が取得でき、悪意のある犯罪者や組織がユーザーの行動履歴を容易に追跡できてしまいます。平文で通信がやり取りされるため、その通信に介入してクエリに対して偽の応答を返すことでユーザーのアクセス先を変更する攻撃なども可能です。これらの問題に対処し通信の秘匿性を高める方法として、近年DNSクエリと応答を暗号化された通信経路でやり取りするDNS over TLS（DoT）やDNS over HTTPS（DoH）が標準化されました。

クライアントからのマルウェアサイトやフィッシングサイトへのアクセスや、マルウェア等に感染した端末からのC&Cサーバー等に対するアクセスにおいてもDNSが利用されることにも注意が必要です。これに対応するためにDNS RPZ（Response Policy Zones）を利用し、脅威インテリジェンスと連携して悪意のあるサイトへアクセスするためのDNSクエリに対する応答を無効化する方法が考えられています。

DNS over TLSとDNS over HTTPSの実現

A10ネットワークスのA10 Thunderシリーズを DNSサーバーの前段に配置することで、既存のDNSサーバーの構成を変更することなく、DoTやDoHを実現できます（図1）。この構成ではA10 ThunderがDoTやDoHを用いたDNSクエリを終端し、TLSやHTTPSによる暗号化通信を復号した後に後段のDNSサーバーに通常のDNSクエリとして転送します。クエリに対する応答はA10 Thunderが暗号化してクライアントへ送信します。A10 Thunderは独自OSや専用ハードウェアの活用により高速な暗号化/復号処理を実現でき、高いTLSオフロード性能を持ちます。これにより、DNSサーバー側ではTLSの処理を行う必要がなくなります。また、DNSサーバーの負荷分散により、DNSの可用性を高めることもできます。後述する各種のDNS向けのセキュリティ機能を併せて利用すると、クエリ/応答の通信の秘匿性を高めるだけでなく、DNSサーバーそのものの防御も併せて実現できます。

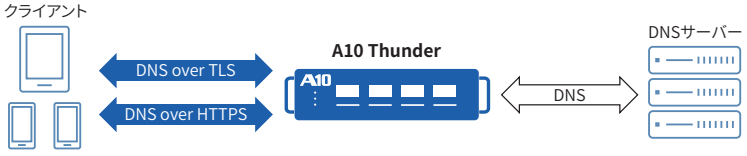

図1：A10 Thunderによる DNS over TLS/HTTPSの実現

課題：

- DNSサーバーの通信経路のセキュリティ強化のためのDNS over TLS（DoT）やDNS over HTTPS（DoH）の実現
- DNSサーバーを利用しているクライアントの悪意のあるサイトへのアクセスの防止
- DNSサーバーそのものへの攻撃やDNSの悪用に対する防御

解決策：

- A10 ThunderシリーズをDNSサーバーの前段で利用し、DoT/DoHを実現
- DNS RPZ（Response Policy Zones）により、悪意のあるサイトに関する名前解決を検知し防御
- DNSクエリのフィルタリング、DNSレスポンスレートリミットなどによるDNSサーバーへの攻撃と悪用に対する防御

メリット：

- A10 Thunderシリーズを導入するだけで既存のDNSサーバーの構成を変更せずにDoT/DoHの実装が可能
- サードパーティの脅威インテリジェンスを利用することで、効果的なDNS RPZを実現
- DNS向けのセキュリティ機能が高性能なサーバー負荷分散やTLSオフロードとの機能と統合されていることによる高セキュリティ・高可用性と高いROIの実現

DNS RPZ への対応

A10 Thunder は DNS RPZ にも対応しており、DNS ファイアウォールとしてクライアントの不正なサイトへのアクセスに伴う DNS クエリを無効化したり書き換えたりすることで、実際のアクセスを止めることができます（図 2）。これによりマルウェアサイトやフィッシングサイトのような不正サイトへのアクセスや、感染した端末からの C&C サーバーへのアクセスをブロックできます。DNS RPZ で利用できるフィードはユーザーが定義して利用するだけでなく、サードパーティ製の脅威インテリジェンスも利用でき、効果的な防御を実現できます。DNS クエリに対し、多様な条件とアクションに基づく柔軟な対応が可能です。

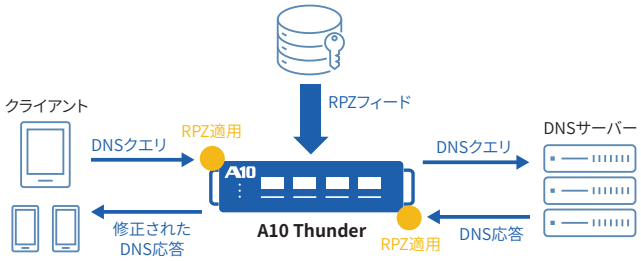

図 2：A10 Thunder での DNS Response Policy Zone（RPZ）の利用

DNS サーバーへの攻撃や悪用に対する防御

アプリケーション配信コントローラ（Application Delivery Controller; ADC）の機能や DNS アプリケーションファイアウォールの機能が併せて利用できることも、A10 Thunder を DNS サーバーの前段に配置する利点となります。ADC の機能によって以下が実現できます。

- DNS サーバーの負荷分散による高可用性や高速なレスポンスの実現
- DNS 応答のキャッシュによる DNS サーバーの負荷軽減
- 後段の DNS サーバーがダウンした際や不完全な応答を返す場合の Thunder 自身による権威 DNS サーバーへの再帰問い合わせによるサービスの可用性の維持
- コネクションレートの制限による不正な大量アクセスからの防御
- ブラックリストに基づく不正な IP アドレスからの接続拒否
- 接続元となる DNS サーバーの認証による不特定多数からのアクセス制御
- DDoS 攻撃防御機能による不正な DNS クエリや DNS アンプ攻撃に対する防御
- DNS クエリのフィルタ機能による、指定したクエリタイプのリクエストのドロップ

また、A10 Thunder CFW を利用することで、ADC 機能に加えて L4 ステートフルファイアウォール機能を併せて利用でき、DNS サービスに対するアクセスのセキュリティをさらに強化できます。最新の脅威情報がリアルタイムで提供される脅威インテリジェンスサービスなどと連携することで、C&C サーバーやオープンリゾルバなどの不正な IP アドレスからのアクセスを効果的に防御できます。

A10 Thunder は前述した独自 OS や専用ハードウェアを利用することで、コンパクトな筐体でも非常に高いサーバー負荷分散性能、ファイアウォール処理性能を有します。また、これらの機能を 1 つの筐体で提供することで、ラックスペースや電力消費、利用するリソースなどが抑えられ、ランニングコストを抑えることができ、高い ROI に繋がります。仮想インスタンスやコンテナでも利用でき、1 つの仮想インスタンスやコンテナで 100Gbps 以上のスループットを実現できます。

まとめ

A10 Thunder を利用することで、インターネットの利用拡大やクラウドサービスの活用において一層重要性が増している DNS のインフラに対する効果的なセキュリティ強化を実現できます。DNS までの通信経路を暗号化する DoT や DoH に対応できるだけでなく、DNS RPZ の利用により不正サイトへのアクセスや不正なクライアントからのクエリを防止でき、各種の DNS セキュリティ機能を併用することで DNS サーバーそのものへの攻撃や DNS の悪用を防御できます。A10 Thunder に集約された ADC 機能やファイアウォール機能との併用により高速な DNS レスポンスや高可用性の実現、DDoS 攻撃に対する防御も併せて実現できます。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）は、サービス事業者やクラウド事業者および企業で利用される 5G ネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。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 117 か国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。

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

Part Number: A10_SB_DNS　Oct 2021