ソリューションブリーフ

DNS over HTTPS（DoH）による DNSトラフィックのセキュリティ確保

中間者攻撃を防ぎDNSクエリのプライバシーを確保

DNS基盤のセキュリティは、サービス事業者やその顧客である企業において、今までさほど重要視されていませんでした。しかし、昨今のDDoS攻撃や、ランサムウェア、データ窃盗攻撃の多くは、DNSを標的として実行されています。その原因の大部分は、DNSクエリが暗号化されておらず、クリアテキストで送信される点にあります。DNSクエリは、DNSクライアントとインターネット上のアドレスを提供しているローカルDNSサーバーとの間で送受信されるリクエストです。他の機密性のあるユーザー情報（パスワード、クレジットカード情報、電子メールアドレスなど）は、通常安全なHTTPSプロトコルを使用して送信されるのに対し、DNSクエリには、この安全な手法が使用されていませんでした。その結果、DNSクエリは簡単にスプーフィング、インターセプト、ハイジャック(乗っ取り)されるリスクがあります。

IETFは、この脆弱性の打開策として、HTTPSによる暗号化を用いて、DNS通信を行うDNS over HTTPS (DoH)を提案しました。Microsoft、Google、Cloudflareなどの企業と、ChromiumおよびMozillaが、この機能を提供しているか、将来サポートを予定しています。

DoH機能をネイティブでサポートしたA10 Thunder® CFWを利用することにより、サービス事業者などの組織は、加入者向けにDNS over HTTPS(DoH)サービスを提供することができるようになります。このソリューションは、サービス事業者の本番環境で既に導入されており、DNS基盤で必要とされるハイパフォーマンスと低遅延を実現しつつ、暗号化によってDNS通信を保護しています。

このソリューションブリーフでは、DoHの利点と、A10ネットワークスが提供するDoH機能について概説します。

課題

DoHは、長年にわたるDNSの脆弱性を軽減して、DNSを利用した攻撃に対するより堅固なセキュリティを加入者に提供します。しかしその一方で、DoHの導入によって、多くの重要な加入者向けサービスが利用できなくなってしまったり、サービス事業者のネットワークパフォーマンスが低下したり、加入者のユーザー体験の制御が難しくなってしまう可能性もあります。

ソリューション

A10 Thunder CFWがネイティブサポートしているDoHと、従来からサポートしているDNSセキュリティ機能とを組み合わせることで、サービス事業者規模のDNS基盤に必要とされるハイパフォーマンスを維持しつつ、DNSクエリの完全な保護を実現することができます。

利点

ケーブル会社や、モバイル通信事業者、ISPは、A10ネットワークスのDoHを使用することで、強固なセキュリティを必要とする加入者に対して、市場で既に稼働実績のあるキャリアクラスのDoHソリューションを提供できます。

課題：考慮すべきDoHの利点と欠点

DoHは、DNSの脆弱性に関する業界の懸念に対処可能

DNSはインターネットの基礎であり、DNS基盤は、ほぼ間違いなく通信事業者にとって最も重要なコンポーネントの一つです。DNSは大量のクエリを処理できるように設計されていますが、様々な攻撃でよく標的にされています。サービス事業者のネットワークとインターネット自体が正しく機能するためには、強靭でハイパフォーマンスなDNS基盤が不可欠です。サービス事業者のネットワーク上での通信セッションは、全てインターネットアドレスを要求する最初のリクエストから始まります。しかし、HTTPSを使用して暗号化されるクレジットカード、電子メール、パスワードなどのユーザー情報とは違って、DNSクエリ/レスポンスの通信は暗号化していないクリアテキストで行われます。その結果、多数のDDoS、ランサムウェア、マルウェア、およびデータ窃盗攻撃で、DNSが悪用される事態になっています。

IETFは、DNS関連のサイバー攻撃に関する懸念の増大に対応するため、DNS over HTTPS（DoH）技術と呼ばれる標準をRFC 8484で提案しました。DoHは、エンドデバイスとローカルDNSリゾルバとの間の通信パスを、ユーザートラフィックのプライバシーを保護するために通常使用されているものと同じプロトコル（HTTPS）を使用して暗号化します。この技術は、従来よりも強力なセキュリティでDNSクエリを保護する一方で、サービス事業者にいくつかの課題を突きつけます。

加入者向けサービスでDNSの使用を困難にするDNSの暗号化

サービス事業者は、DNSクエリの内容に基づいて、マルウェア対策ツール（悪意のあるサイトへのユーザーアクセスのブロック/検知）や、ペアレンタルコントロール、コンテンツフィルタ、低遅延ビデオコンテンツ配信、法的調査、セルフインストールなど、多くの重要なサービスを提供しています。ケーブル事業者や、モバイル通信事業者、ISP、他のサービス事業者が提供している付加価値サービスの多くは、加入者がデフォルトでDoHを使用するようになると、機能しなくなる可能性があります。モバイルネットワークのパフォーマンスは、遅延の増大とDoHのオーバーヘッドによって低下する可能性もあります。

DNS over HTTPS（DoH）機能を備えたA10 Thunder CFW

従来よりも強固な保護を加入者に提供すると同時に、DNSを使用したサービスの制御を維持

モバイル通信事業者や、ケーブル事業者、ISP、他のサービス事業者は、A10ネットワークスが提供する、市場で実証済みのハイパフォーマンスソリューションを採用して自社のDNS基盤にDoHを付け加えることで、DNSクエリの制御とDNS情報の可視性を維持しつつ、誤ってサービスが中断することを防ぐことができます。Tier-1事業者によってテストされ、本番環境に導入されたA10のソリューションは、数十億のDNSクエリをサポートしています。サービス事業者はこのソリューションによって、DNS基盤の働きを妨げず、DNSを使用したサービスの制御を維持したまま、DoHの使用を要求する加入者に、この機能を提供することができるようになります。先進的なDNSロードバランシングや、DNSキャッシュ、DNS保護などの機能を含むA10の包括的なDNSソリューションは、世界中のサービス事業者の物理ネットワークと仮想ネットワークの両方に導入されています。DoHは、このDNSソリューションの拡張機能であり、すでにTier-1事業者のネットワークに導入され、数十億のDNSクエリを処理しています。

サービス事業者は、A10 Thunder CFWのDoH機能によって、DNSクエリのエンドツーエンドの暗号化を通じた強固なセキュリティとプライバシー保護向上という選択肢を加入者に提供できます。サービス事業者は、DNS情報を使用する付加価値サービス（マルウェア対策ツール、ローカライズされたビデオコンテンツ配信、ペアレンタルコントロールを含むフィルタなど）を提供する能力を維持することができ、法規制にも対応できます。これによって加入者との関係がさらに強化され、加入者が他のDNSプロバイダを使用することにより、提供しているサービスから誤って離れてしまうことを防ぐことができます。

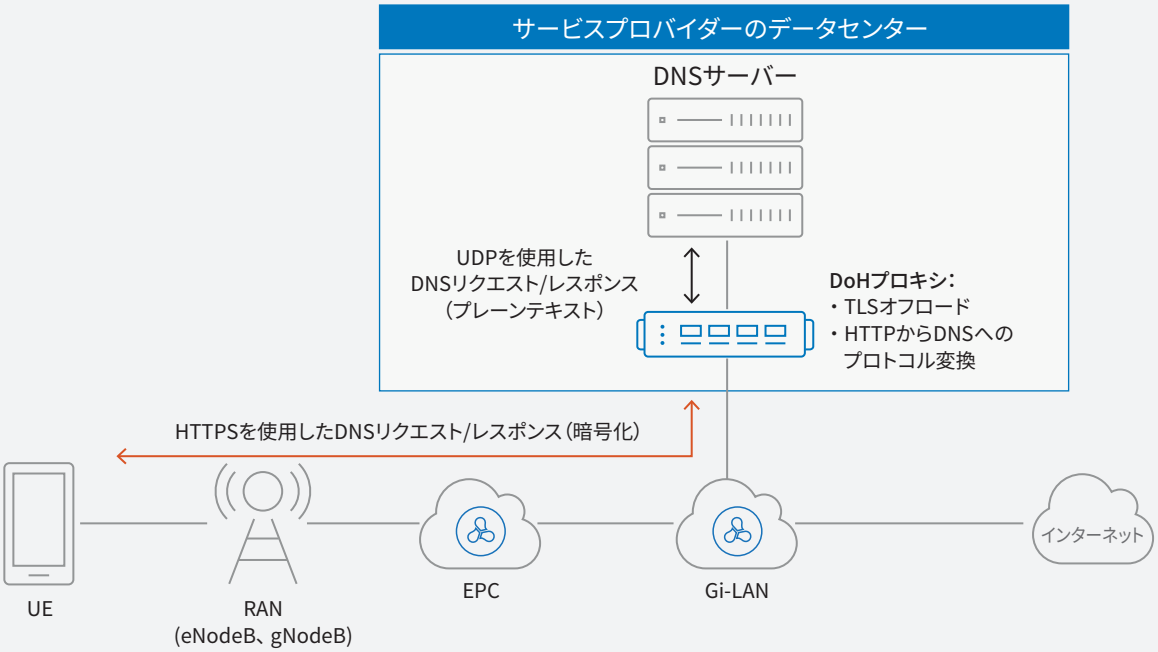

図1: モバイルサービス事業者のネットワークにおけるHTTPSを使用したDNS

特長

DoHは、ハードウェアや仮想アプライアンスを含むすべてのA10 Thunder CFWアプライアンスでネイティブ機能として提供されているため、環境にあわせて、任意のフォームファクタでの導入が可能です。A10ネットワークスのAdvanced Core Operating System®（ACOS）のネイティブ機能であるDoHを、アプリケーションデリバリーコントローラー（ADC）などのA10 Thunder CFWの他のセキュリティ機能と組み合わせて使用することで、サービス事業者規模のDNS基盤に必要とされるパフォーマンスを維持しつつ、DNSの包括的な保護と可用性を提供することができます。

大規模な本番環境で実証済みのDoH機能を持つA10 Thunder CFWは、ユーザープライバシーの確保と中間者攻撃からの保護を提供しつつ、サービス事業者が期待しているピーク時数百万、1日数千億のクエリを低遅延で処理する能力を提供します。A10のソリューションは業界標準RFC 8484/1035に完全準拠しています。

DoHには以下のような利点があります。

導入コストの削減： A10 Thunder CFWのDoH機能は、サービス事業者の既存DNS基盤への投資を保護しつつ、機能強化できるように設計されています。A10 Thunder CFWを導入することで、既存のDNS基盤の構成を変更することなく、セキュアな接続性とプロトコル変換機能を迅速に提供できるようになります。A10 Thunder CFWには、5G対応製品群「A10 Orion 5G Security Suite」の構成要素であるADCの全機能を含む、複数のセキュアアプリケーションサービスも含まれています。

拡張性と高い性能： TLSにより実施されるDoH暗号化では、高い処理能力が必要になります。A10 Thunder CFWは、大量のDNSクエリとDoHトラフィックの処理に必要な拡張性とパフォーマンスを考慮して設計されています。暗号化処理に特化した専用ハードウェアにより、大量の暗号化されたDNSクエリを処理できます。

セキュリティと可視性： A10 Thunder CFWの既存機能であるセキュアアプリケーションサービスを併せて使用することで、DoH機能を拡張することが可能となっており、サービス事業者は、要件に応じて複数のサービスを組み合わせて利用することができます。既存機能には、DNSアプリケーションファイアウォールや、DNSリクエスト、クエリのレート制限、DNSフラッド攻撃防御、DNSキャッシュなどがあり、DNS基盤のセキュリティ、可用性、パフォーマンスを向上させることができます。

ソリューションの構成要素

- 本番環境で実証済みの技術
- DoH、HTTP/2のネイティブサポート
- HTTPからDNSプロトコルへの変換
- RFC 8484、1035準拠
- 全てのDNSタイプ、IPv4/IPv6クエリのサポート
- 数百万の顧客、数十億のDNSクエリをサポートした通信事業者での実績
- A10 Thunder CFWで利用可能
- A10 Thunder CFWが提供するネットワーク機能やセキュリティ機能と同時に使用可能

既存DNS基盤をDoHで迅速に強化

DNS over HTTPS（DoH）は提案中の標準ですが、GoogleやMozillaなどのWeb業界におけるトップ企業が強力にサポートしたため、短期間で市場に浸透しました。サービス事業者は、現在の設定構成を変更せずに、既存のDNS基盤にDoH機能を迅速に追加することができます。サービス事業者は、DoHサービスを利用する加入者の制御を維持しつつ、DNSを使用する付加価値サービスが誤って「停止」してしまうことを防ぐことができます。これにより、保護を強化する一方で、加入者のユーザー体験を向上させることが可能になります。

お問い合わせ

詳細については、下記をご覧ください。
https://www.a10networks.co.jp/products/thunderseries/thunder-cfw.html

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：http://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

©2020 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networks は米国およびその他各国における A10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。
商標について詳しくはホームページをご覧ください。www.a10networks.com/a10-trademarks

Part Number: A10-SB-19207-JA-01　APR 2020