ソリューションブリーフ

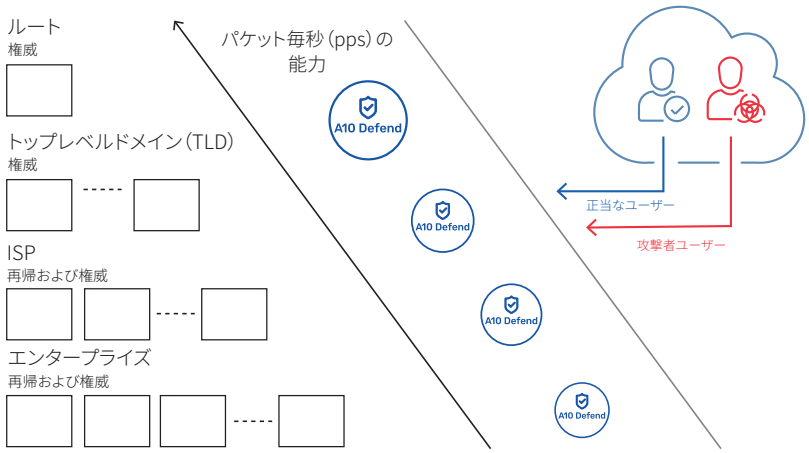
マルチベクトル型DDoS攻撃に対する耐性強化

重要なDNSインフラストラクチャを保護

概要

DNS（ドメインネームシステム）は、ユーザーが円滑にインターネットを閲覧するためにサービスプロバイダや企業にとって重要なインフラストラクチャです。ウェブサイトやインフラストラクチャを標的にした大規模な分散型サービス妨害（DDoS）攻撃は最近のニュースでも注目され、高い信頼性が求められるインターネットサービス、およびDNSの停止に伴い大きな打撃を与えることからDNSの重要性の認識が大きく高まっています。
ネットワーク事業者は積極的に、DDoS攻撃の耐性を備えたDNSインフラストラクチャを構築し、十分な防御を施さなければ、予測できない結果を被ることになります。

A10 Defendはあらゆる規模のDNSインフラストラクチャを保護



課題

DNSはすべてのユーザーにとってインターネットアクセスに不可欠で重要なシステムです。攻撃者がビジネスオペレーションを中断させるために最も標的とするサービスの1つです。

ソリューション

A10 Defendは、あらゆる規模のビジネスサービスの可用性を保証しマルチベクトル型DDoS攻撃に適したDDoS対策ソリューションです。費用対効果に応じてさまざまなフォームファクタで利用可能です。

特長

- マルチベクトル型DDoS攻撃に最適な耐性強化策を提供
- テラビットレベルの規模や、対策が困難な巧妙なDDoS攻撃からDNSを保護
- 正常なトラフィックの挙動を自動的に学習
- 攻撃対応時のリスク軽減策を自動化し効率的に防御
- オープンAPIでオーケストレーション機能を統合しセキュリティ運用を単純化

DNSの脅威の全体像

DNSインフラストラクチャに対するDDoS攻撃は非常に単純です。正当なユーザーと同様、攻撃者はインターネットを介してDNSにクエリを送信し、DNSはレスポンスを返します。問題は、攻撃者が大規模なボットネットを利用し、DNSに過剰な負荷をかける時に発生します。

正当なユーザーと攻撃者を識別して不正な活動を阻止し、円滑な運用を実現するため不可欠なDNS防御と解決すべき課題

- DNSサーバは、大容量のネットワークトラフィック、およびリソース枯渇型のプロトコル攻撃に強くありません。
- 攻撃者はDNSの特性および脆弱性を利用します。
- UDPベースの転送メカニズムのため、攻撃者は送信元IPを簡単に偽装することができます。
- DNSレスポンスの特性は、攻撃者に多くの攻撃機会を与えます。
- 攻撃者はDNSクエリとDNSレスポンスのパケットサイズの大きな差異を利用して増幅攻撃を行います。
- DNSは、何百万ものセキュリティ対策がない公開されたDNSリゾルバからの行われるリフレクション攻撃に強くありません。

攻撃方法

フラッディング

DNSサービスはサーバ上のネットワーク機能で実行されます。結果として、不正な形式のパケット、ランダムポートへのUDPパケット、TCP SYNフラッド、および他のリソース枯渇型の攻撃など、一般的なネットワークフラッド攻撃の影響を受けます。攻撃者はボットネットを利用して、大量の不正なトラフィック、つまり大量の不正なDNSクエリを送信して、正当なユーザーが利用するサーバを停止させます。

スプーフィング（なりすまし）

DNSクエリのなりすましは、通常、コネクションレス型のUDP経由で行われるため、非常に簡単です。攻撃者は自身のIPアドレスからクエリを送信する代わりに、任意のIPアドレスに偽装してDNSクエリを送信し、攻撃元を隠蔽し、より効果的かつ大規模な攻撃を行うことができます。

モノのDDoS

脆弱で常時接続したIoT（モノのインターネット）デバイスが兵器と化した結果、より広範囲に分散されたデバイスで構成されるボットネットから攻撃することが可能になりました。兵器化したIoT機器は、DNSサーバに偽のトラフィックを氾濫させ、攻撃対象のDNSサーバのリソースを枯渇させ、正当なユーザーに対してDNSの再帰機能および権威機能が十分に提供できなくなります。

DNSリフレクション（反射）・アンプリフィケーション（増幅）

リフレクション（反射）の動作を利用し送信元のアドレスを標的のIPアドレスになりすまし、DNSリクエストとレスポンスパケットサイズの差異を利用して攻撃トラフィックを増幅させます。攻撃者は、世界中の公開されたDNSリゾルバサーバに対して、偽装した多数のリクエストを送信し、標的となる権威サーバのリソースを枯渇させます。効果を最大化するため、リフレクション（反射）攻撃は非常に大きなDNSレスポンスを生成するように増幅するDNSプロトコルの特性を利用します。

ランダムクエリ（水攻め）攻撃

ランダムクエリ（水攻め）攻撃は無効または存在しないドメインでDNSクエリを送信します。再帰DNSサーバは、キャッシュにないランダムなクエリを送信することで、権威DNSサーバに存在しないレコードを検索させることでリソースを枯渇させます。また、不要なデータでキャッシュがいっぱいになるため、パフォーマンスが悪化します。

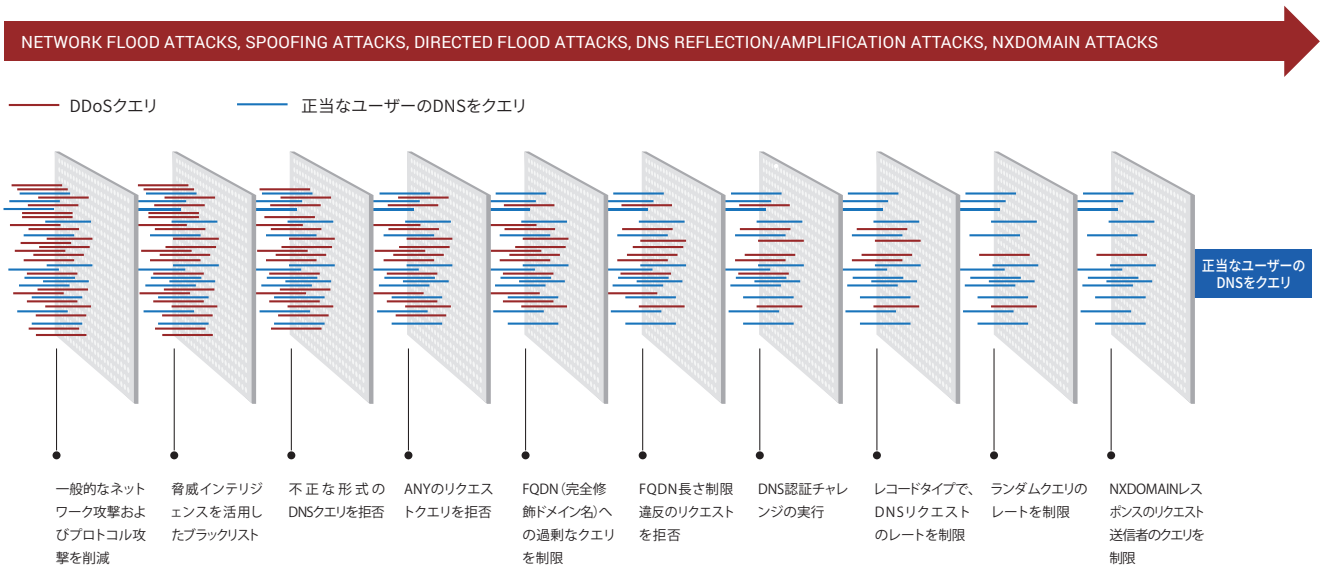
動作の仕組み

A10 Defendはネットワークの境界でマルチベクトル型DDoS攻撃を検知および防御します。IoTを悪用したDDoS攻撃や従来のゾンビPCのボットネットから保護するため、エッジルータやスイッチからのパケットやフローレコードを分析しDDoS攻撃を検出します。これは、学習した正常なトラフィックと比較して異常な挙動を検知するため27以上のトラフィック挙動インジケータでトラフィックを追跡して、正当なユーザーと攻撃者のボットを正確に区別します。DNSサービスには複数階層の保護が提供されており、ソースベースのレート制限、チャレンジレスポンス認証、不正なリクエストのブロック、ブラックリストの登録などが含まれます。

A10 Defendは、GUI、CLI（コマンドラインインターフェース）から、オープンAPIまで、幅広いカスタマイズ機能を提供します。これにより、防御する側は、カスタマイズできる防御策の構築が可能で、標的型のマルチベクトル型DDoS攻撃に対するDNSサービスの耐性を強化します。

A10 Defend の DNS に対する DDoS の防御

ユーザーと攻撃者



A10 Defend の DNS 防御のコンポーネント

A10 Defend は、一般的なネットワーク攻撃と DNS 固有の攻撃ベクトルの検出とリスク軽減策を提供します。

一般的な DNS サーバのリスク軽減措置

- DNS サーバファームを保護する一般的な対策
- L3/L4 パケットの異常の検出
- 送信元ベースのフィルタリングと制限
- 無効な不正な形式のパケットの検出
- TCP/UDP/DNS 認証チャレンジ
- 宛先ベースのフィルタリングと制限
- 正常なトラフィックの学習とベースラインの設定
- 学習したベースラインのしきい値と比較した、5 段階の自動化リスク軽減策の設定
- 既知の不正なソースをブロックする統合型脅威インテリジェンス

DNS 固有の軽減対策

- 不正な形式のクエリを拒否
  - 基本
  - 拡張
- ANY のリクエストクエリを拒否
  - 実用性が限定的なコストが大きなクエリを制限
- FQDN 長の制限違反リクエストを拒否
  - 任意のサフィックスの位置
  - 特定のサフィックスの位置で開始
- FQDN（完全修飾ドメイン名）への過剰なクエリを制限
  - 送信元 IP 単位
  - 評価する FQDN のラベル数を指定（最大 10）
- レコードタイプで、DNS リクエストのレートを制限
  - 高度な攻撃から防御
- NXDOMAIN レスポンスのリクエスト送信者のクエリを制限
- 宛先のクエリレートを制限
  - サーバへの過剰な負荷を防止
- 送信元 IP 毎に DNS クエリ認証チャレンジを実行
  - 時間制限ありの強制リトライ
  - TCP レスポンスへ強制的に切り替え

これらのリスク軽減策機能により、増幅型、Land 攻撃、水攻め攻撃、およびファントムドメイン攻撃などの DDoS 攻撃から防御します。これらは DNS 攻撃の中で最も一般的な攻撃で DNS サービスに対して大きな影響を与えます。

リスク軽減策の自動化エスカレーション機能

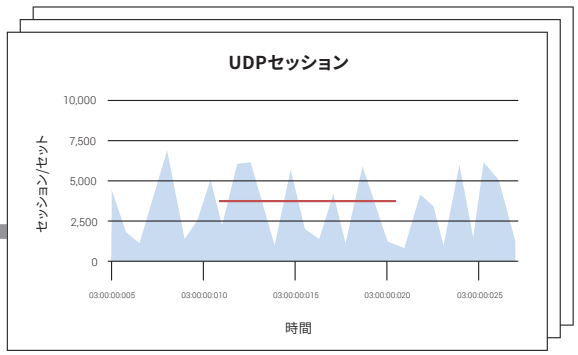
攻撃対応時の混乱の中、熟練したスタッフやリソースを無制限に使える組織はありません。A10 Defend は、保護するゾーンやサービス単位で、学習済の正常時のベースラインと比較して、5 段階レベルのプログラマチックなリスク軽減策の引き上げおよび引き戻しをサポートしています。管理者は、保護するサービス単位に調整したポリシーを作成することで、A10 Defend は各レベルで必要なリスク軽減策を自動的に適用します。これにより、時間がかかる現場スタッフの手作業による変更が不要になり、攻撃時における対応時間が短縮します。

管理者は、特定の段階で、手動で介入することもできます。

DNS 防御のリスク軽減策のエスカレーションポリシーの例

	インジケータの追跡	*リスク軽減措置の適用*	*アクション*
レベル 4 - 攻撃対応時 最終的な対策	インジケータの追跡を継続 ゾーンしきい値 4	BGPブラックホールシグナリング 管理者の手動介入 すべてのレベル3のリスク軽減措置	カスタム正規表現を作成 カスタムのBerkley Packet Filterを作成
レベル 3 - 攻撃対応時 対策の改善	インジケータの追跡を継続 ゾーンしきい値 3	DNS-udp-authentication-force-tcp Dst-rate-limit-request すべてのレベル2のリスク軽減措置	課題 拒否 宛先レートの制限 送信元をブラックリストに登録
レベル 2 - 攻撃対応時 対策の改善	インジケータの追跡を継続 ゾーンしきい値 2	DNS-udp-authentication-force-retry Malformed-DNS-query-check-extended Src-rate-limit-by-request-type すべてのレベル1のリスク軽減措置	課題 拒否 ソースのクエリタイプのレートの制限 送信元をブラックリストに登録
レベル 1 - 攻撃対応時 対策の追加	インジケータの追跡を継続 ゾーンしきい値 1	Malformed-DNS-query-check-basic DNS-any-check FQDN-label-length FQDN-rate-limit-domain-name-suffix FQDN-label-count すべてのレベル0のリスク軽減措置	拒否 FQDNのチェック 送信元レートの制限 送信元をブラックリストに登録
レベル 0 - 正常時 ベースラインの設定、 最小限の対策	TCP-conn-miss-rate TCP-pkt-drop-ratio TCP-syn-rate TCP-src-threshold TCP-zone-threshold UDP-pkt-drop-ratio UDP-pkt-rate UDP-src-threshold UDP-zone-threshold	L3/L4パケットの異常性チェック	拒否

各レベルへの自動引き上げ
および引き戻し用に27以上の
インジケータを追跡



保護するサービスの
挙動ベースラインを設定

機能と特長

- マルチベクトル型 DDoS 攻撃からの完全な保護
- 27 以上のトラフィック挙動インジータを追跡し正規のユーザーとボットネットを高精度に識別
- コネクションレート単位で送信元と宛先の組み合わせによる詳細な保護策
- 迅速な応答、検出とエスカレーション措置の間隔を200msに短縮
- 能力を300Gbps、440Mppsにスケールし、単一のアプライアンスで同時に追跡するセッション数を1億2800万にスケール
- ポリシーエンジンは100%APIを使ったプログラムが可能で、自動オーケストレーションとのインテグレーションが容易
- ネットワークに導入が容易なオンデマンド型のリアクティブ方式の導入、およびBPG、OSPF、IS-ISルーティングを使用したL2/L3のプロアクティブ方式の導入が可能

次のステップ

A10 Defend 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いただくか、以下のサイトをご覧ください。

http://a10networks.co.jp/products/thunderseries/thunder-tps/index.html

まとめ

新しい脅威は範囲、強さ、複雑さにおいて変化しています。非効率なシグネチャベースのIPSやトラフィックのレート制限に依存する既存のソリューションでは、もはや十分に対抗できません。A10 Defend は、最も難しいDNSベースの攻撃を防御するためのスケーラビリティと正確性を備え、DDoS攻撃に対するDNSインフラストラクチャの耐性を強化します。

古い世代のDDoS製品とは異なり、A10 Defend は市場で実績あるA10のACOS®（Advanced Core Operating System）プラットフォームをベースにしています。そのため、拡張可能なフォームファクタと経済的なコスト構造で完全な防御、検知、報告が可能です。

A10は、A10 DDoSインシデントセキュリティ対応チーム（DSIRT）を含め、24時間365日、DDoSのインシデントや攻撃の分析および対応のサポートを行っています。A10脅威インテリジェンスサービスは、世界中の知識を活用して、既知の攻撃リソースからプロアクティブに保護します。

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-19175-JA-03 JUN 2024