radware

Smart Network. Smart Business.

重要なDNSインフラストラクチャの防御

ラドウェアアタック・ミティゲーション・システム(AMS) - ホワイトペーパー

目　次

はじめに

あらゆるWebトランザクションには、インターネットサービスプロバイダが提供するDNSサービスが必要不可欠です。そのため、DNSはインターネットの根幹を支える重要なインフラストラクチャと言えます。攻撃がDNSサービスを中断させることに成功すると、その他すべてのインターネットベースのサービスが停止してしまいます。

通信事業者やサービスプロバイダはさまざまな攻撃防御ツールを使用していますが、現在のDNSインフラストラクチャは依然として脆弱です。多様化を続ける攻撃はこれまで以上に巧妙になっており、軽減することが困難になっています。したがってDNSサービスを保護するためには、DNSサービスに対する新種の攻撃を検出、防御する専用ツールを用いて、境界セキュリティを検討し直す必要があります。

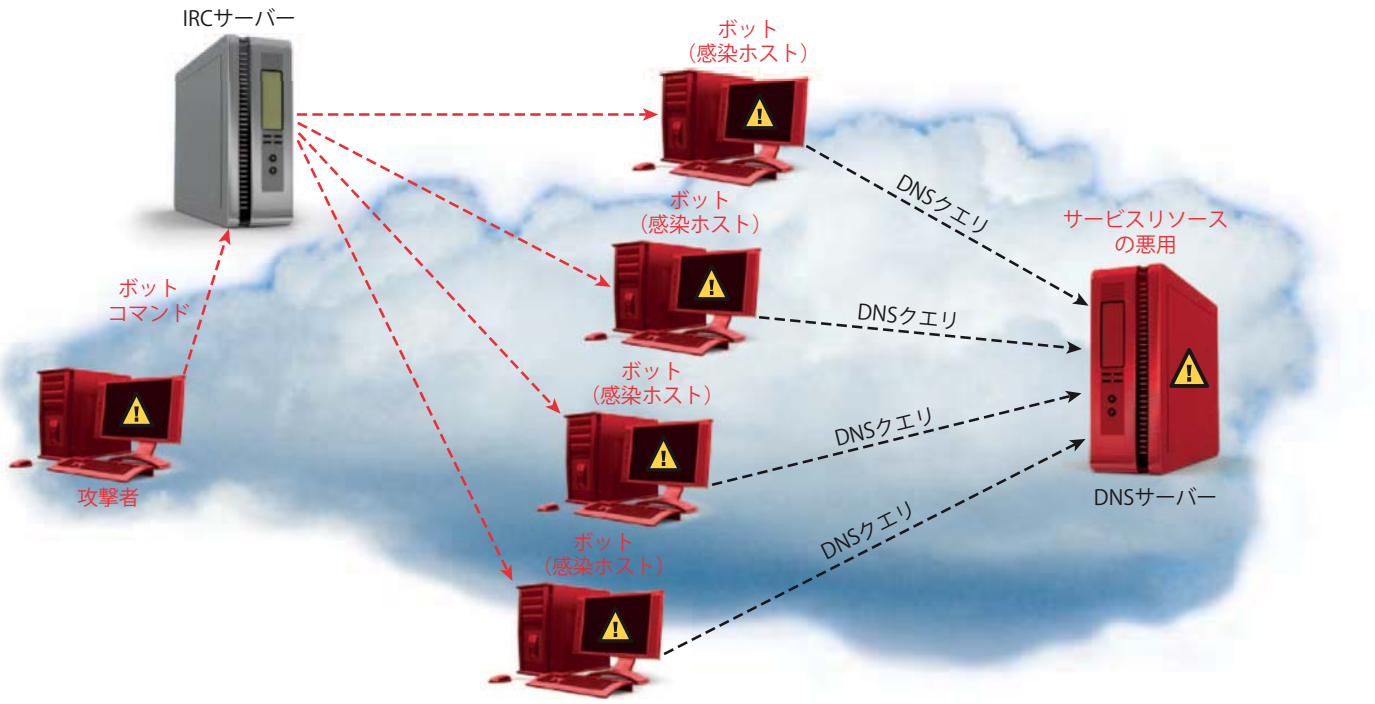
本ホワイトペーパーでは、DNSサービスに対する最近のDDoS攻撃の詳細と、このような攻撃を防御するという課題について説明します。また、ラドウェアのDNS DDoS攻撃防御ソリューションが、DNSサービス攻撃に対する比類なき世界最高の攻撃防御ツールである理由について説明します。

DNS DDoS攻撃の増加と進化

すべてのWebトランザクションにおいて、要求されたWebサイトにアクセスする際にはホスト名からIPアドレスを得るためにDNSクエリを必要とします。このため、DNSは通信事業者やサービスプロバイダに不可欠なインフラストラクチャです。サービスプロバイダにとってDNSサービスの遅延や中断は、インターネットベースのサービスに対して即時に影響を与え、正規ユーザーがインターネットにアクセスできなくなってしまいます。攻撃者は、サービスプロバイダがDNSインフラストラクチャを保護するセキュリティ対策を取っていることを理解しています。そのため、サービスにより深刻なダメージを与えるために、さらに巧妙な攻撃を生み出しています。

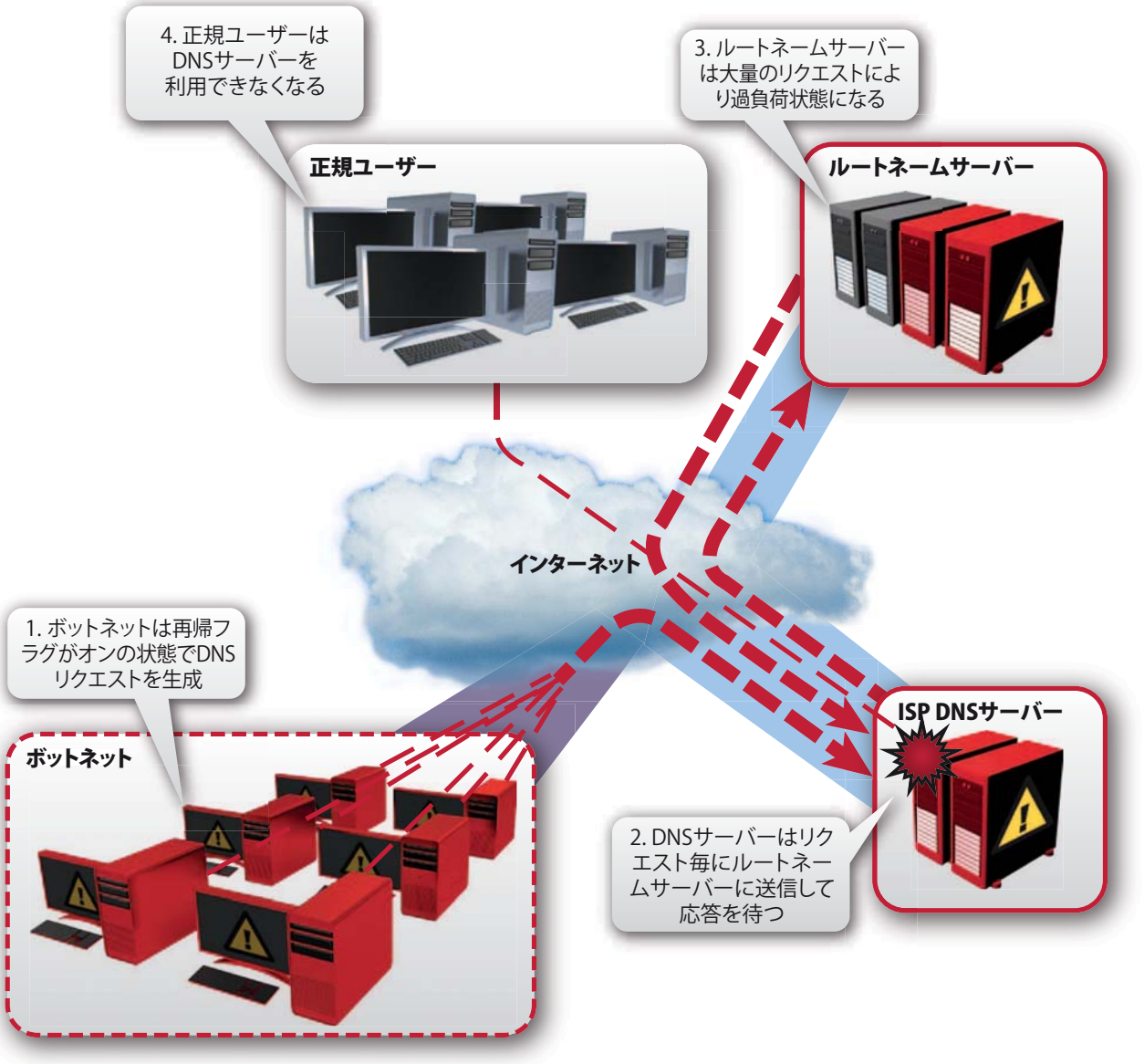
このセクションでは、DNSサービスを中断させようとする攻撃者が仕掛ける、最近の攻撃手法について説明します。

- **DNSフラッド攻撃** — 攻撃者はボットネットと呼ばれる複数の感染ホストを踏み台として利用することで、大量の処理負荷を与えるDDoS攻撃を仕掛け、DNSサーバーを機能停止へ追い込みます。DNSサービスでは主にUDPを使用して通信が行われるため、大量の負荷を与える攻撃をより受けやすいと言えます。また、DNSの規格に従ってDNSサーバーは全てのリクエストを処理するために、高負荷を引き起こしてしまいます。そのため、攻撃者はこの特徴を悪用して、驚くほど少数のボットでもDNSサービスにダメージを与えることができてしまいます。



- **DNS増幅攻撃（Amplification Attack）**— 標準的なDNSリクエストのサイズは、本来DNSリプライよりも小さくなります。DNS増幅攻撃では、攻撃者はより大きいリプライを得るためにDNSクエリを入念に選択します。また得られるリプライは時によりリクエストに比べ最大80倍大きいものになります。このため、「通常の」DNSフラッド攻撃と比べて、DNSサーバーにより高い負荷を与えます。

- **DNS再帰攻撃（Recursive Attack）**— これはDNSフラッド攻撃の増幅手法のひとつです。分散化された大量のDoS攻撃によりDNSサーバーをフラッドさせます。この攻撃では、攻撃者はDNSクエリパケット内の再帰フラグをオンにします。再帰フラグがオンになると、DNSサーバーはリクエストを別のサーバーにリダイレクトせずに、強制的に自身でホスト名の解決を実行し、送信者に応答を返す動作となります。DNS再帰攻撃では、攻撃者はDNSクエリごとにリクエストするドメイン名をわずかに変更します。そのため、DNSサーバーはキャッシュされた結果で応答することができず、ドメイン名を何度も調べることになります。このようにDNSサービスに負荷を与え続け、最終的には正規ユーザがサービスを利用できなくなります。



DNS再帰攻撃の図解

DNS DDoS攻撃から保護するための課題

先述のとおり、DNSサーバーへのDDoS攻撃はますます複雑化してきているため対応が困難になっています。今日の攻撃防御ツールはDNS攻撃を効果的に防ぐため、以下の課題に対処していく必要があります。

防御ツールによるDNSトラフィックの振る舞い分析 — 巧妙な攻撃者は、DNSプロトコルの特徴を悪用し、DNS再帰攻撃などDNSサービスに大きくダメージを与えるようなより強力な攻撃を行います。こうした攻撃を防御するには、DNSプロトコルについての深い知識に基づき、DNSトラフィックの振る舞いを的確に理解し、プロトコルの各フィールド毎に注意深く分析する必要があります。

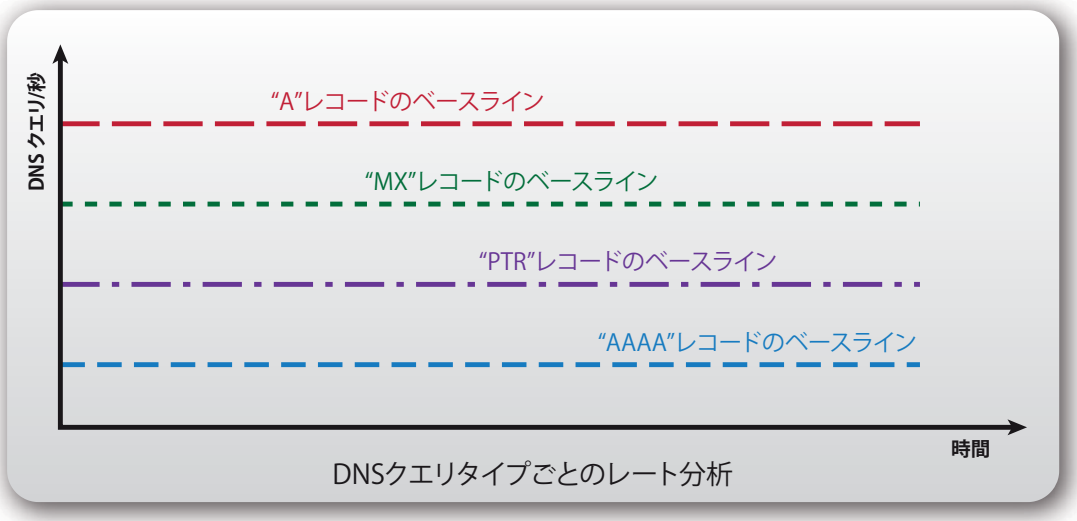
高レートのDNSパケットの防御 — DNS DDoS攻撃には大量かつ高レートのフラッドパケットが伴います。攻撃防御デバイスは、すべての攻撃パケットを防ぐために、大量のトラフィック（通常、数百万パケット/秒）を処理しなければなりません。一方で正規のDNSトラフィックを処理するために十分な帯域を提供する必要もあります。

正確な防御 — 正規のDNSトラフィックと攻撃DNSトラフィックの識別に失敗すると、正規ユーザーがインターネットサービスにアクセスできないなどの誤検知を引き起こします。インターネットサービスプロバイダにとって誤検知の影響は非常に大きく、企業評価の低下や収益損失などにつながります。そのため、今日の攻撃防御ツールは正確に攻撃を判別し、攻撃下でも正規ユーザーにはサービスを提供しなければなりません。

攻撃を受けている間も良好なユーザーエクスペリエンスを提供 — 攻撃防御ツールは正確さに加え、攻撃を受けても正規ユーザーに良好な体感品質を継続して提供する必要があります。攻撃防御ツールは限りなく低遅延の処理が求められます。そのため、ソフトウェア処理のみのデバイスではなくハードウェアエンジンやアクセラレータにより構成されるデバイスで提供する必要があります。

DNS DDoS攻撃に対するラドウェアのソリューション

DNS　DDoS攻撃に対するラドウェアのソリューションは、DNSフラッドプロテクション機能により提供されます。この機能は、定評あるDefensePro製品ラインのBehavioral DoSモジュールの一部です。DNS攻撃防御ソリューションは、検出フェーズ、リアルタイムシグネチャ作成フェーズ、防御フェーズという3つのフェーズに分けられます。

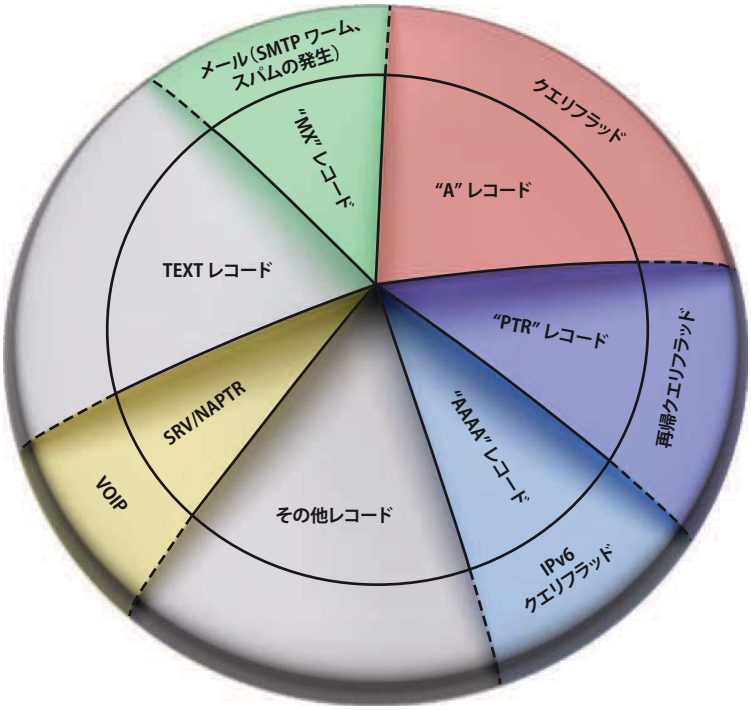


DNSクエリタイプごとのレート分析

検出フェーズ

検出フェーズでは、DefenseProはUDPポート53上のすべてのインバウンドDNSトラフィックを監視して、正常なDNSトラフィックの振る舞いとしてベースラインを学習します。各DNSクエリに対して、クエリタイプ毎にベースラインを更新します。これは、クエリレートならびにレートに依存しない全DNSクエリに対する相対割合になります。

さらに、ファジーロジックエンジン[1]を使用して、継続的に攻撃度合いのスコアを計算します。ファジーロジックモジュールは、リアルタイムのネットワークデータと現在のベースラインの評価に基づいて、リアルタイムに攻撃を検出する多次元分析エンジンです。攻撃度合いのスコアが攻撃とみなされる値を超えると、システムは防御フェーズに移行します。



DNSクエリ分散分析

リアルタイムシグネチャ作成フェーズ

DefenseProはDNS DDoS攻撃を防御するために、リアルタイムシグネチャを自動生成して、人手を介することなくDNS DDoS攻撃を防ぎます。ベースライントラフィックから逸脱したリアルタイムトラフィックのサンプルを使用して、疑わしいトラフィック内において発生しているアノマリに特有のパラメータを検出します。

自動シグネチャ作成モジュールの分析に用いられる代表的なパラメータタイプは以下のとおりです。

- パケットチェックサム
- パケットサイズ
- パケットID
- TTL（Time to Live）
- フラグメントオフセット
- 送信元IPアドレス
- 送信先IPアドレス
- ポート番号
- DNS Qname - ドメイン名
- DNSクエリID - クエリ識別番号
- DNSクエリカウント（Qcount）

これらのパラメータの値が「異常」としてフラグが立てられると、システムは疑わしいパラメータに基づいてリアルタイムシグネチャを作成し、「クローズドフィードバックループ」と呼ばれるシグネチャ最適化メカニズムを有効にします。

クローズドフィードバックモジュールは、最も厳密かつ効果的なシグネチャブロッキングルールを作成する役割を担います。疑わしいフラグの立てられた各パラメータは、自動シグネチャ生成メカニズムによって検出された値を複数含むことができます。クローズドフィードバックモジュールは、AND/OR論理演算を使用してこれら複数の最適な組み合わせを決定します。異なる値とパラメータタイプ間により多くのAND論理関係が構築されるほど、より正確かつ厳密なシグネチャブロッキングルールとみなされます。検出されたシグネチャ値の間に論理関係を構築するために、クローズドフィードバックモジュールは以下のようなフィードバックを使用します。

- **ポジティブフィードバック:** クローズドフィードバックモジュールにより作成されたシグネチャブロッキングルールによって、トラフィックアノマリが低減されたことを示します。さらに同様のアクションを行い、できる限り多くのAND条件を使用し、より多くの攻撃に特有のパラメータ（シグネチャタイプと値）を組み合わせます。

[1] ラドウェアのファジーロジックエンジンについて詳しく知るには、http://www.radware.com/Thank_you_download.aspx?ID=5557（英文ページ）をダウンロードしてください。

- **ネガティブフィードバック:** トラフィックアノマリの度合いが変わらない、もしくは増加したことを示します。直近で作成したシグネチャブロッキングルールの使用を停止し、より適切なルールを継続して探していきます。
- **攻撃停止フィードバック:** 攻撃が終了した場合、即座にすべての防御手段を停止します（シグネチャルールを削除します）。

リアルタイムシグネチャは、次のフェーズで疑わしいトラフィックに対して適用されます。

防御フェーズ

防御フェーズでは、DefenseProはリアルタイムシグネチャを利用してDNS攻撃の疑わしい送信元を検出し、攻撃を停止するために次のエスカレーション・ステップを実行します。

エスカレーション・ステップ#1:シグネチャベースのチャレンジ – DefenseProは、リアルタイムシグネチャにマッチするDNS AおよびAAAAクエリに対してチャレンジ（詳細は次ページの図を参照）を行います。チャレンジの目的は、正規ユーザーによって作成された正規トラフィックと、ボットネットによって生成されたDoSトラフィックとを識別するために行われます。

エスカレーション・ステップ#2:シグネチャベースのレート制限 – エスカレーション・ステップ#1の後においても、クローズドフィードバックモジュールが依然として攻撃の継続を確認している場合、DefenseProは次のエスカレーション・ステップに移行します。このステップでは、リアルタイムシグネチャにマッチするDNSトラフィックに対してレート制限を実施します。

エスカレーション・ステップ#3:全トラフィック・チャレンジ – このステップでは、疑わしいソースからだけでなく、すべてのユーザーからの全DNS AおよびAAAAクエリトラフィックのチャレンジを行います。ここでも、チャレンジの目的は、正規ユーザーによって作成された正規トラフィックと、ボットネットによって生成されたDoSトラフィックとを識別するために行われます。

エスカレーション・ステップ#4:全トラフィック・レート制限 – なおも攻撃が継続している場合は最終手段のエスカレーション・ステップとして、定義済みの最大クエリレートに従って、すべてのDNSトラフィックに対してレート制限を実行します。

リアルタイムシグネチャとDNSチャレンジは、DoS Mitigation Engine（DME）というハードウェアアクセラレータによって適用されます。これにより、正規トラフィックに影響を与えずに数百万パケット/秒の攻撃トラフィックを処理することを可能にします。

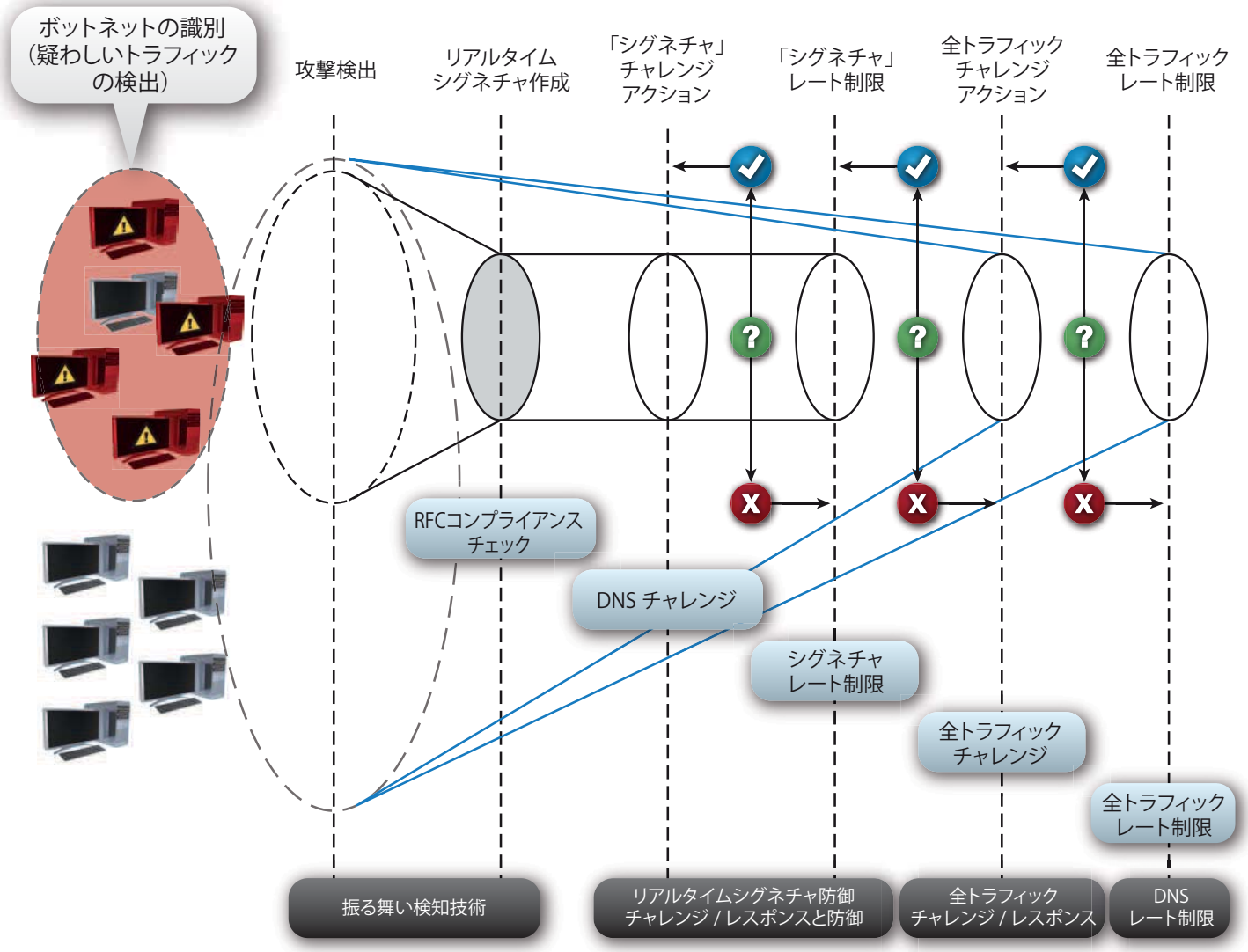
DNSチャレンジと選択的破棄メカニズム

上述のエスカレーション・ステップの間、DefenseProは、DNS送信元が攻撃者ではなく、正規ユーザーであることを確認するために**DNS**送信元にチャレンジを行います。チャレンジは、クエリタイプAおよびAAAAに対して行なわれ、RFC定義に基づいています。このチャレンジでは、DefenseProはDNS送信元から受信する最初のパケットを無視します。

DNSの規格に従い、新しい同一のDNSパケットは同一識別番号を使用し3秒以内に再送されなくてはなりません。DNS送信元に対するチャレンジやチャレンジに対する応答を検証するために、DefenseProは統計テーブルと関数を使用し、選択的破棄メカニズム（SDM ; Selective Discard Mechanism）を実行します。SDMテーブルの各エントリでは、テーブルに到達した各クエリのスコアが計算されます。送信元がチャレンジに正しく応答すると、そのスコアは増加し、内部DNS認証テーブルに登録します。一方、送信元がチャレンジに正しく応答しない場合、そのスコアは減少します。

ユーザーエクスペリエンスへの影響を最小化するために、チャレンジ動作が実行されている間は、防御モジュールは認証テーブルを使用し、チャレンジに正しく応答した送信元IPアドレス情報を一定期間、保持します。

送信元プロキシデバイスに関して、正規ユーザかもしくは攻撃者かを誤って判別しないように、SDMはモジュールに新たに到達しチャレンジされていないクエリの送信元スコアを減少させます。送信元のスコアが一定の値を下回ると、再度チャレンジが行なわれます。チャレンジに対して適切な応答が得られた場合、送信元のスコアは増加し、以降のクエリにはチャレンジを行いません。



チャレンジ/レスポンスとアクション・エスカレーション

DefenseProのDNS攻撃防御の3フェーズ

DNS DDoS攻撃防御ツールの課題に対処するDefensePro

先述のとおり、攻撃を効率的に防ぐためには、DNS DDoS防御ツールはいくつかの固有の課題に対処する必要があります。DefenseProは、これらの以下の課題すべてに対処することのできる業界初のDNS DDoS攻撃防御製品です。

防御ツールによるDNSトラフィックの振る舞い分析 ― DefenseProはDNSトラフィックを理解し、その正常な振る舞いを継続的に学習し、異常なDNSトラフィックを即座に識別します。さらにDNSトラフィック内の各フィールドを分析することにより、異常なパケットを検出し正確なリアルタイムシグネチャを生成します。

高レートのDNSパケットの防御 — ネットワークプロセッサベースのハードウェアアクセラレータであるDMEにより、DefenseProは、200万DNSクエリ/秒にチャレンジでき、最大1200万パケット/秒の攻撃トラフィックを処理します。攻撃トラフィックがDefenseProの正規トラフィックを処理する機能に影響を与えることはなく、攻撃を受けている間もマルチギガビットのパフォーマンスを提供します。

正確な防御 — 独自のDNSチャレンジ・メカニズムとDNSトラフィックの正確な振る舞い分析により、DefenseProは誤検知を最小限に抑え、正規DNSトラフィックと攻撃DNSトラフィックを正確に判別します。このため、サービスプロバイダは深刻な攻撃を受けても、正規ユーザーにサービスを継続して提供することができます。

攻撃を受けている間も、良好なユーザーエクスペリエンスを提供 — DefenseProは複数のハードウェアエンジンとアクセラレータにより構成された独自のアーキテクチャにより、すべての処理トラフィック、特に正規トラフィックに対して最小の遅延時間を保証します。上述のDNSチャレンジは、攻撃トラフィックの疑いのあるソースに対してのみ、リアルタイムシグネチャを適用します。これにより、攻撃を受けても正規インターネットユーザーに良好なユーザーエクスペリエンスを保証します。

まとめ — 世界最高のDNS DDoS攻撃防御ツール

DefenseProは、世界最高のDNS DDoS攻撃防御ツールです。独自の特許技術とチャレンジ機能により、巧妙かつ大規模なDNS DoS攻撃を完全に防御します。

DefenseProは攻撃を防御するだけでなく、攻撃を受けている間も正規ユーザーに良好なユーザーエクスペリエンスを提供します。これは攻撃者と正規ユーザーを正確に識別することにより実現します。

DefenseProは独自の検出および防御フェーズに加え、4つの攻撃防御エスカレーション・ステップを実行します。これらの機能により、重要なDNSインフラストラクチャを保護するために、業界初の完全なDNS DDoS攻撃防御ソリューションを提供します。