データシート

サービスプロバイダ向け Infoblox Advanced DNS Protection

課題：サービスの中断

CSP、モバイルオペレーター、クラウドプロバイダーはすべて、DNS に大きく依存しています。これは、一部は重要な接続コンポーネントとして、また一部は暗黙的または明示的に顧客に提供するサービスとして利用されています。CSP は、自社の評判のため、そして安定した常時接続のインターネット接続に依存する顧客のために、この重要な資産を保護しなければなりません。DNS サーバーがダウンすると、サブスクリプション加入者はインターネットから切断されます。DNS の中断により、メール、Web サイト、VoIP、SaaS（Software as a Service）などの重要な IT アプリケーションへの干渉やシャットダウンが発生します。

主要なセキュリティレポートによると、DNS はアプリケーション層攻撃の標的として 2 番目に多いサービスであり、2018 年には企業の 72% が影響を受けました。Neustar は、DNS を介して分散した多数の端末が連携して実行する DDoS 攻撃によって生じるコストは、サブスクリプション加入者の離脱やブランドへの損害を除いて、1 時間あたり 22 万ドルを超えると見積もっています。攻撃者はネットワーク内の最も脆弱なリンク（攻撃ベクトル）を探しますが、DNS プロトコルは DDoS や DNS ハイジャックに簡単に悪用され、このような攻撃は DNS の完全性を侵害します。

多層的な防御に残る盲点

多くの CSP ネットワークは、侵入防止システム（IPS）、ファイアウォール、ロードバランシングシステムなど、プロバイダーのインフラストラクチャのさまざまな側面を保護するのに優れたツールを採用しています。しかし、これらのツールは DNS サーバーと統合されておらず、DNS の理解や可視性がないため、DNS に適用しても効果がありません。

これらのツールを広範囲に導入しているにもかかわらず、多くの CSP は、DNS への攻撃については、依然としてネットワークパフォーマンスの低下やその他の劣化について顧客から報告を受けたときに初めて気付くと不満を漏らしています。ほとんどの組織では、DNS システムへの攻撃に関する早期警告はほとんど、あるいはまったくありません。多くの運用チームは、トラフィックレベルが上昇したかどうか、サーバーが負荷を受けているか、または侵害されているかを判断するために、DNS サーバーのログデータを手動で解析することさえしています。

保護が必要な重要領域

プロバイダーのネットワーク内で保護が必要な 2 つの重要な領域は、権威 DNS サーバーと DNS キャッシュ・サーバーです。プロバイダーのネットワーク内のさまざまな場所にある権威 DNS サーバーは、サブスクリプション加入者ベースからの DNS クエリと接続要求に応答します。権威ある DNS サーバーは、オンラインプレゼンス、電子商取引機能、モバイル IP 接続のための複数のネットワークコ

利点と機能

ビジネスの中断を軽減：
Infoblox Advanced DNS Protection（ADP）は、あらゆる種類のDNS攻撃（ボリューム型攻撃、DNS エクスプロイト、DNS ハイジャックなどの非ボリューム型攻撃を含む）を継続的に監視、検出、阻止し、正当なクエリに応答します。また、DNS ハイジャック攻撃によって侵害される可能性のある DNS の整合性を維持します。Infoblox は、ネットワークに 99.999% の可用性を実現する強固なセキュリティ基盤を提供します。

進化する脅威への適応：
Infoblox ADP は Infoblox Threat Adapt™ テクノロジーを使用し、新しい脅威や進化する脅威が出現すると、それに対する防御を自動的にアップデートします。Threat Adapt は、Infoblox の脅威スペシャリストが顧客のネットワークで確認したものなど、進化する攻撃手法に対して独自の分析とリサーチを適用し、保護をアップデートします。また、DNS の設定変更を反映して、自動的に保護を適応させます。

ンポーネントの位置特定を可能にし、特に LTE および 5G ネットワークにおけるローミングとゲートウェイの位置特定を支援します。サブスクリプション加入者のインターネット体験を円滑にするにあたり、DNS キャッシュ層は、DNS クエリに迅速に応答する上で重要な要素です。したがって、許容可能な応答時間を実現するためには、頻繁にアクセスされる Web サイトやその他の URL のクエリ応答をキャッシュに保存することが重要です。

新しい変数：暗号化された DNS

新しく登場した暗号化 DNS 標準は、DNS 要求のプライバシーと応答の整合性を保護する一方で、CSP は暗号化 DNS サービスを提供しない限り、ネットワーク内での DNS 使用を管理するために必要な制御の一部を失う可能性があります。DNS over TLS（トランスポート層セキュリティ）または DoT、および DNS over HTTPS（DoH）は、オペレーティングシステムのスタブリゾルバまたはローカルアプリケーションと再帰的 DNS リゾルバ間の DNS 通信を暗号化することによって機能します。両方の技術は、DNS クライアントとサーバー間の通信を暗号化することにより、データのプライバシーと認証を確保します。しかし、その際、多くのソリューションが外部の DNS リゾルバーを指すように変更され、クライアントデバイスがプロバイダーの制御外の DNS サービスにアクセスできるようになり、サブスクリプション加入者は潜在的なセキュリティリスクや顧客体験の悪化にさらされます。プロバイダーは、これらのテクノロジーがもたらすリスクを軽減するために、今すぐ対策を講じる必要があります。ネットワークに DNS リゾルバーを介して暗号化を実装することで、サブスクリプション加入者のネットワーク体験を制御し続けることができます。これにより、プロバイダーはセキュリティ、コンテンツフィルタリング、その他の重要なオンネットサービスを引き続き提供することが可能になります。

解決策：DNS ベースの攻撃による障害からビジネスを守る

Infoblox Advanced DNS Protection（ADP）を使用すると、ビジネスを常時稼働し続けることができます。DNS ベースの攻撃を受けている間も例外ではありません。Infoblox は、ボリューム型攻撃、NXDOMAIN 攻撃、脆弱性攻撃、DNS ハイジャックなど、非常に広範な攻撃も阻止します。インフラのオーバープロビジョニングや単純な応答率制限に依存するアプローチとは異なり、ADP は常に更新される脅威情報を活用し、セキュリティパッチを展開する必要なく、適切なクエリにのみ対応しつつ、DNS 攻撃をスマートに検出・軽減します。Infoblox を使用すると、重要なネットワーク・インフラストラクチャとビジネスを常に運用し続けるようにすることで、ネットワークの信頼性を次のレベルに引き上げることができます。

暗号化された DNS 標準に対応

Infoblox Network Identity Operating System（NIOS）は、Infobloxのコアネットワークサービスを支えるOSであり、ネットワークインフラストラクチャの継続的な運用を確保します。Infoblox Encrypted DNS for Service Providers は、Infoblox が提供する最高クラスの DNS と付加価値的なサブスクリプション加入者サービスを提供しつつ、効率的な暗号化を実現する NIOS 機能です。DoT および DoH をサポートする Infoblox Encrypted DNS は、DNS トラフィックを暗号化するための独自のアプローチを提供します。ロードバランサーやオーバープロビジョニングに依存する方法とは異なり、Infoblox Encrypted DNS は、すべての DNS ニーズに対応する単一のサービスとして機能します。ADP の仮想化インスタンスを通じて利用できる Infoblox Encrypted DNS により、Infoblox はエンドポイントがサポートするプロトコルに関係なく、エンドポイントと DNS サーバー間のラストマイル DNS 通信を暗号化できます。この機能をサポートすると同時に、暗号化された DNS 通信に関連する追加諸経費によるパフォーマンスの懸念も解決します。同じサービスから、他の DNS 機能がすべて実行されている間に接続がすでに確立されている場合、CSP はマイクロ秒の遅延で暗号化された DNS に対応できます。

利点と機能

単一画面での可視性を獲得：
Infoblox を使用することで、通信サービスプロバイダー（CSP）は過去または現在の DNS 攻撃を簡単に確認し、迅速な脅威の軽減を通じて運用効率を向上させることができます。Infoblox Advanced DNS Protection は、ネットワーク全体の攻撃ベクトルと攻撃の発生源に関する単一のビューを提供し、脅威管理に必要なインテリジェンスを供給します。これは、当社の DNS ソリューションに統合されています。

柔軟な導入：
通信事業者は Infoblox Trinzic Flex 仮想アプライアンスを導入できます。これにより、通信事業者は弾力的な拡張機能とサービスプロバイダーに合わせた容量ベースの価格設定を活用しながら、Infoblox のフットプリント全体に特定の機能を追加することが可能となります。

コストを削減する：
Infoblox Software ADP は既存のハードウェアを活用するため、お客様に求められるのはハードウェア上で実行されるソフトウェアをアップグレードすることだけで、これによりアップグレードの追加コストは最小限に抑えられます。

柔軟な展開オプション

Infoblox Advanced DNS Protection は、スケーラブルなエッジ展開を必要とする CSP 環境向けに設計されています。オーケストレーションされた仮想化ネットワーク機能（VNF）やクラウドネイティブ・ソリューションなど、複数のキャリアグレードのオプションで利用できます。

- **Infoblox Trinzic Flex：**仮想マシンに割り当てられたリソースに基づくスケーラブルな仮想プラットフォームです。Infoblox Network Identity Operating System（NIOS）は仮想マシンの容量を自動的に検出し、適切なプラットフォームにスケーリングします。さらに、Trinzic Flex アプライアンスは Service Provider License Agreement Program（SPLA）の対象となっています。
- **物理プラットフォームおよび仮想プラットフォームで利用可能：**Software ADP は、Trinzic TE-815/825/1415/1425/ 2215/2225/4015/4025 アプライアンスのソフトウェアサブスクリプション・アドオンです。

攻撃名	タイプ	仕組み
DNS リフレクション / DDoS攻撃	ボリュメトリック	サードパーティの DNS サーバー（オープンリゾルバー）による DoS または DDoS 攻撃の伝播
DNS アンプ攻撃	ボリュメトリック	特別に作成されたクエリを使用して増幅された応答を作成し、被害者にトラフィックを大量に送信
TCP/UDP/ICMP フラッド攻撃	ボリュメトリック	大量のトラフィックでネットワークまたはサービスをダウンさせることによる、レイヤー 3 でのサービス妨害
NXDOMAIN	ボリュメトリック	DNS サーバーに存在しないドメインへのリクエストが大量に送信され、キャッシュが飽和状態になり、応答時間の遅延が発生
ランダムなサブドメイン（水責め攻撃）、ドメインロックアップ攻撃、ファントムドメイン攻撃	低ステルス性	攻撃の一環として設定された架空または不正なドメインへのリクエストで DNS サーバーを氾濫させ、リソースの枯渇、キャッシュの飽和、送信クエリ制限の枯渇、パフォーマンスの低下を引き起こします
DNS ベースの脆弱性攻撃	脆弱性攻撃	DNS ソフトウェアの脆弱性を悪用した攻撃
DNS キャッシュポイズニング	脆弱性攻撃	不正なアドレスで DNS キャッシュデータを破損
プロトコル異常	脆弱性攻撃	不正なパケットやクエリを送信してサーバーの停止が発生
偵察	脆弱性攻撃	ハッカーが大規模な DDoS またはその他のタイプの攻撃を開始する前にネットワーク環境に関する情報を取得しようとする試み
DNS ハイジャック	脆弱性攻撃	ドメイン登録情報を上書きして不正な DNS サーバーに指定する攻撃
データ窃取（既知のトンネルを使用）	脆弱性攻撃	攻撃は、DNS ポート 53 を通じて別のプロトコルをトンネリングすることを含みます。これは、ファイアウォールが非 DNS トラフィックを許可するように設定されている場合に可能であり、データの持ち出しを目的としています。

表 1: 高度な DNS 保護（ADP）が防御する攻撃タイプの概要

サブスクリプション加入者とブランドの保護

サービスプロバイダー向けの Infoblox キャリアグレードソリューションは、グローバルな脅威インテリジェンスと自動化された保護パッケージを使用して、サブスクリプション加入者を保護します。これらのソリューションは、急速に進化するネットワーク、増加するトラフィック、さらには悪意のある DDoS 攻撃中でも、重要な DNS サービスの可用性を維持します。

- Infoblox Advanced DNS Protection は、サービスプロバイダーの DNS インフラストラクチャ向けに業界で最も包括的かつ統合された DNS 保護ソリューションです。
- 増幅、リフレクション、プロトコル異常、トンネリングなどの DNS ベースの攻撃に対する高度な自動検出および軽減機能がすべて DNS サーバーに組み込まれています。
- キャリアグレードで、オーケストレーションされた仮想化ネットワーク機能（VNF）やクラウドネイティブソリューションを含む複数のフォームファクターで利用可能であり、世界最速のDNSキャッシュサーバーを特徴とし、DNSキャッシュと権威DNSデプロイメントをサポートします。
- Infoblox からの自動更新による脅威インテリジェンスおよび緩和ルール。
- 特許取得済みの Infoblox Grid™ テクノロジーは、広範な制御、自動化、および更新の配信を提供し、運用サポートコストを削減し、手動構成エラーによる停止のリスクを排除します。
- DNS over TLS（DoT）および DNS over HTTPS（DoH）などの暗号化された DNS プロトコルをサポートします。

詳細については、
www.infoblox.com/spまたはお近くの Infoblox 担当者にお問い合わせください。

Infoblox はネットワークとセキュリティを統合して、比類のないパフォーマンスと保護を提供します。Fortune 100企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に検知・対処できます。

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com/jp