データシート

暗号化された DNS を用いた連邦のサイバーセキュリティ強化

ホワイトハウスの大統領令に準拠した、暗号化された DNS の実装

概要

最近のガイダンスにおいて、ホワイトハウスは国家のサイバーセキュリティを強化し促進することを目的とした包括的な大統領令（EO）を発行しました。この EO は、ソフトウェアおよびクラウドサービスプロバイダーの説明責任を改善し、連邦政府の通信および ID 管理システムを強化し、行政部門および機関全体で新興技術の使用を促進することにより、サイバーセキュリティを強化することを目指しています。特に、導入された主要な対策の中には、DNS トラフィックの機密性と整合性を確保するための暗号化された DNS プロトコルの要件があります。これにより、DNS は最前線の重要なセキュリティ制御として認識され、サイバーセキュリティの多層防御戦略におけるその重要性が強調されています。

最近の連邦政府のサイバーセキュリティに関する命令に従い、Infoblox Advanced DNS Protection（ADP）は暗号化された DNS トラフィックを強力にサポートし、DNS 通信の機密性と整合性を確保します。この機能は、サイバーセキュリティ対策を強化し、ホワイトハウスが発表した暗号化 DNS に関する最新の大統領令に準拠することを目指す連邦政府機関にとって不可欠です。

Infoblox のソリューションは包括的で、拡張性があり、実装が簡単であるため、中断を最小限に抑えて暗号化された DNS へのスムーズな移行が可能です。重要なのは、15 を超える米国の連邦民間機関が、Advanced DNS Protection に含まれる Infoblox DNS 暗号化を利用していることです。この採用は、ゼロトラスト・イニシアチブを支援するために DNS 暗号化を有効にすることで、ゼロトラストセキュリティポリシーの義務化を進める上で役立っています。

エージェンシーの課題

暗号化された DNS は、DNS メッセージの送受信時に暗号化と復号化を行う必要があるため、特に DNS サーバーで追加のコンピューティングリソースを必要とします。政府機関は、暗号化されたDNSの広範な展開を開始する前に、これを予測し、DNS サーバーにクエリ負荷を処理するために十分なリソースがあることを確認する必要があります。暗号化された DNS が適切に実装されない場合、ネットワーク全体、そのアプリケーション、およびユーザーに損害を与える可能性があります。

暗号化された DNS は、ネットワークトラブルシューティングツールを使用する IT スタッフが DNS クエリや応答の内容にすぐにアクセスできないため、トラブルシューティングをさらに困難にする可能性があります。DNS クエリと応答の内容は、ネームサーバー自体で IT スタッフが引き続き利用可能です。これは、これらのネームサーバーは必要な復号化を実行しているからです。

主な機能

サイバーセキュリティの義務を支援
最新の連邦サイバーセキュリティガイドラインを確実に遵守します。

暗号化された DNS トラフィックのサポート
安全で認証された DNS 通信を実現するために、DNS over HTTPS（DoH）および DNS over TLS（DoT）をサポートします。

高度な脅威保護
NIOS およびクラウドテナントのアドレスブロックとルーティング領域を定義および管理します。

高速クエリロギングパフォーマンスに大きな影響を与えることなく、DNS トラフィックをリアルタイムでキャプチャし、ログに記録します。

スケーラブルで信頼性が高い
卓越したスケーラビリティと信頼性により、大量の DNS および DHCP トラフィックを効率的に管理します。

これらの課題を克服し、サイバーレジリエンスを確保するために、機関は 1 つのシステム上で複数のミッションクリティカルなサービスの共存を制限する必要があります。計算要件の増加を考慮すると、この職掌分散は可能な限り最高の回復力を提供します。DNS サービスをホストするインフラストラクチャは、そのタスク専用にし、この目的のために強化して、攻撃対象領域を減らし、DNS サービスに対して十分なシステムリソースが利用できる状態を確保する必要があります。インフラストラクチャには、ログ記録、暗号化された DNS プロトコルのサポート、プロテクティブ DNS などの DNS サービスの要素に対応できる十分な容量が含まれている必要があります（該当する場合）。これは、専用の DNS サービスで、サービスとして、または仮想アプライアンスや物理アプライアンスを介して実現する方が簡単かもしれません。

INFOBLOX ADVANCED DNS PROTECTION

安全な DNS ソリューションのリーダーとして、Infoblox は連邦政府機関がこれらの新しい要件を満たすにあたり、これを支援する独自の立場にあります。Infoblox Advanced DNS Protection（ADP） は、Infoblox Trinzic ハードウェアおよびソフトウェアアプライアンスに追加可能なソフトウェア・サブスクリプションです。DNS over HTTPS（DoH）やDNS over TLS（DoT）などの暗号化 DNS プロトコルをサポートし、オンプレミスおよびクラウド環境の両方に適しています。さらに、ADP は、DDoS 攻撃、マルウェア、データ持ち出しなど、多様な脅威から DNS インフラストラクチャを保護するための包括的なセキュリティ・ソリューションです。同機関は、オンプレミス、プライベートクラウド、パブリッククラウド環境を問わず、DNS の整合性を保護し、外部および内部からの DNS DDoS 攻撃を防止できます。

暗号化された DNS トラフィックのサポート

- DNS over HTTPS（DoH）：ADP は、DNS トラフィックを HTTPS 経由で実行する DoH をサポートし、HTTPS の広範な普及とセキュリティを活用して DNS クエリと応答を保護します。
- DNS-over-TLS (DoT)：ADP は、トランスポート層セキュリティ (TLS) を使用して DNS トラフィックを暗号化する DoT もサポートしています。このプロトコルは、DNS 通信が安全であり、認証されていることを保証します。

高度な脅威保護

ADP は、高度な脅威インテリジェンス、自動化された脅威軽減、DNS トラフィックのリアルタイムの可視性を提供し、DNS サービスの整合性と可用性を保証します。

- ボリューム型攻撃や非ボリューム型攻撃（DNS エクスプロイトや DNS ハイジャックなど）を含む、あらゆる種類の DNS 攻撃を継続的に監視、検出、阻止し、同時に正当なクエリに応答します。
- 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 ADP は、Threat Adapt™ テクノロジーを活用して、独立した分析と調査を用い、新たな脅威に対する保護を自動的に更新し、DNS 構成の変更に適応します。

高速クエリおよび応答のロギング

ADP には、DNS トラフィックをリアルタイムでキャプチャして分析するために不可欠な、高速 DNS クエリと応答のログ記録が含まれています。高速かつ軽量な設計で、パフォーマンスを大幅に犠牲にすることなく、DNS トラフィックをキャプチャして記録するための迅速かつ柔軟な方法を提供します。

- I/O集約型のクエリおよび応答のログ記録とは異なり、dnstapは非同期で動作し、パフォーマンスの低下を最小限に抑えつつ、高速なクエリログ記録を可能にします。
- dnstap を使用して、柔軟なバイナリ構造のログ形式で DNS サーバーから直接情報をバッファリングし、その後、このデータを受信サーバーにストリーミングします。
- 諸機関はビッグデータツールを活用してこのデータを分析し（他のソースと組み合わせて）、ネットワーク使用パターンの包括的なイメージを構築できます。

スケーラビリティと信頼性

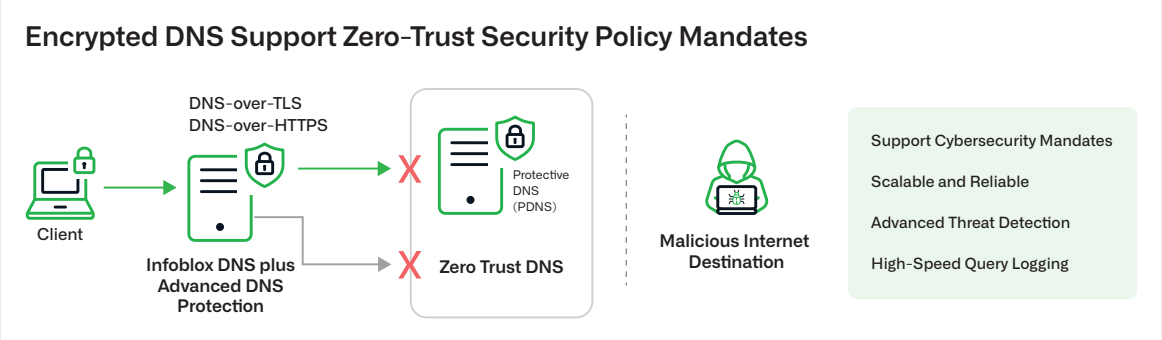
最新の Infoblox Trinzic アプライアンスは、優れた拡張性と信頼性を提供するように設計されており、厳しいネットワーク要件を持つ連邦機関に最適です。

- Infoblox の最新のネットワークにおけるイノベーションとおよびセキュリティの進歩を活かし、将来のネットワーク需要を支えるように設計されています。
- DNS クエリ数（QPS）と DHCP リース数（LPS）のパフォーマンスが 1 秒あたり 50% 向上し、大量の DNS および DHCP トラフィックを効率的に管理できます。
- 分散アーキテクチャ全体での容易な導入と管理により、ネットワークのレジリエンスとスケーラビリティを確保します。
- Infoblox の Cloud Platform（CP）API、DNS Firewall（DFW）RPZ サポート、および DNS Traffic Control（DTC）統合グローバルサーバー負荷分散の以前にライセンスされた機能が含まれています。

導入オプション

- ADP は拡張性が高く、導入が容易で、DNS インフラストラクチャを保護することで機関のサイバーセキュリティ体制を強化する上で役立ちます。諸機関は、ADP 機能を有効にした Infoblox DNS サーバーを導入し、暗号化された DNS トラフィックのサポートを実装できます。
- このデプロイメントはオンプレミス、クラウド、またはハイブリッド環境で行うことができるため、さまざまな運用ニーズに対応する柔軟性を提供します。

Infoblox が貴社の組織における暗号化 DNS の導入を支援する方法についての詳細は、Infoblox チームに scsprogram@infobloxfederal.com または担当のアカウント担当者に直接お問い合わせください。



コール・トゥ・アクション

連邦機関は、最近のホワイトハウスの大統領令に応じて、Infoblox Advanced DNS Protection (ADP) を導入し、DNSセキュリティを優先するよう求められています。この命令は、DNS を重要な最前線のセキュリティ制御として認識し、暗号化された DNS プロトコルの使用を義務付けています。ADP を実装することにより、機関は DNS トラフィックの機密性と完全性を確保し、潜在的なサイバー脅威から保護することができます。Infoblox の包括的かつスケーラブルなソリューションは、DNS-over-HTTPS および DNS-over-TLS をサポートしており、暗号化された DNS への移行をシームレスかつ効果的に行うことができます。

Infobloxはネットワークとセキュリティを統合して、これまでに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

バージョン：20250203v1