内部ドメインのクエリがUmbrellaインサイトに記録されない理由の理解

内容

はじめに

このドキュメントでは、内部ドメインのクエリがログに記録されない理由について説明します。

概要

仮想アプライアンス(VA)を含むUmbrella Insightsを使用する場合、すべてのワークステーションは、VAを指すDNSサーバ設定のみを持つ必要があります。 既存の内部DNSサーバを使用するようにVAを設定する必要があります。 ダッシュボードでは「内部ドメイン」のリストを入力できるため、クライアントが内部リソースに対してDNSクエリーを実行すると、VAが要求を内部DNSサーバの1つに転送します。 時折、これらの内部要求がロギングに表示されない理由を尋ねられます。

説明

前述のように、VAが受信した内部DNS要求は、セットアップ時にVAで設定された内部DNSサーバのいずれかに転送されます。 これらはコンソールで確認できます。 すべて正常に動作している場合、内部DNSサーバは応答を発行し、VAはこれをクライアントにリレーします。

クライアントは、内部ドメインのリストにないリソースに対してDNS要求を行うと、それを包括エニーキャストIPアドレスに転送します。 この要求には、リゾルバへのDNSクエリに追加のデータが含まれており、要求を送信元に結び付けることができます。 送信元には、ユーザIDハッシュ、送信元IP、またはこの拡張DNSパケットに含まれるその他の多数の識別要因などがあります。 この余分なデータは、コマンドラインから特定のDNSクエリを実行することによって確認できます。

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

DNS要求の実際のロギングは、リゾルバで行われます。 ロギングは、この一意の情報がDNSパケットに付加されることに依存します。 VAは、転送するDNS要求をログに記録しません。 最も重要なのは、再帰 DNSサーバです。 パブリックリゾルバがDNSクエリを受信すると、実際のク

エリと一緒に送信された拡張データを使用して、送信元を識別し、適切なポリシーを適用し、要求の情報を口グに記録します。また、要求が許可されたかブロックされたかについてもダッシュボードに表示されます。 内部DNSクエリはリゾルバを認識しないため、リゾルバを口グに記録することはできません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。