セキュアアクセスのためのF5ロードバランサDNS転送設定

内容

お問い合わせ内容

UmbrellaからSecure Accessへの移行中に、F5ロードバランサをクライアントDNSサーバとして使用すると、DNS解決が機能しませんでした。DNS要求が仮想IP(VIP)に到達すると、F5ロードバランサはバックエンドDNSフォワーダにパケットを正常に転送しましたが、エンドポイントマシンでホスト名を解決できませんでした。仮想アプライアンスをクライアントDNSサーバとして直接使用している場合は、DNS解決が正常に機能しました。これは、問題がF5ロードバランサ設定に固有であることを示しています。

パケットキャプチャにより、DNS応答が予想されるF5 VIPアドレスではなく、仮想アプライアンスのIPアドレスを使用していることがわかりました。クライアントコンピュータは、DNS応答がF5 VIPアドレス（MACアドレス）から来ることを期待していましたが、バックエンドの仮想アプライアンスのIPアドレスから応答を受信しました。

環境

- Cisco Umbrellaによるセキュアなアクセス移行環境
- DNSロードバランシングVIPが設定されたF5ロードバランサ
- バックエンドサーバとしての複数のDNSフォワーダ
- DNSサーバとして機能する仮想アプライアンス
- ロードバランサを介したDNS解決を必要とするクライアントエンドポイント

解決策

この問題は、クライアントコンピュータと仮想アプライアンス間のプロキシとして正しく機能するようにF5ロードバランサを設定することで解決されました。主要な設定変更には、自動マップ機能を使用したSource Network Address Translation(SNAT)の有効化が含まれていました。

実行される診断手順

ステップ1:DNS解決動作を確認します。

DNS解決は、問題を切り分けるために、F5ロードバランサVIPと直接仮想アプライアンス接続の両方を使用してテストされました。

ステップ2:DNSトラフィックのキャプチャと分析

パケットキャプチャは、F5ロードバランサを介したDNS要求および応答フローを分析するために実行されました。

ステップ3：送信元アドレスの不一致を特定する

分析の結果、DNS応答にはF5 VIPアドレスではなく、仮想アプライアンスのIPアドレスが含まれていることが判明し、クライアントの混乱を招いていることが判明しました。

設定の変更

手順1:F5ロードバランサ設定にアクセスします

DNS VIP構成を変更するには、F5ロードバランサ管理インターフェイスに移動します。

ステップ2:SNAT自動マップを有効にする

F5ロードバランサで自動マップするようにSNAT(Source Network Address Translation)を設定します。これにより、F5デバイスはクライアントとバックエンドDNSサーバ間のDNS要求および応答を適切にプロキシできます。

手順3：設定を確認します。

SNAT自動マップ設定の実装後、F5ロードバランサを介してDNS解決が正常に機能し始めました。

原因

根本原因は、F5ロードバランサでの不適切なSource Network Address Translation(SNAT)設定でした。SNAT自動マップが有効になっていないと、F5デバイスがDNSトラフィックのプロキシとして正しく動作しませんでした。これにより、想定されるF5 VIPアドレスではなく、仮想アプライアンスのIPアドレスを送信元として使用して、バックエンドの仮想アプライアンスからクライアントコンピュータにDNS応答が直接送信されるようになります。クライアントコンピューターは、要求の送信先と同じIPアドレス(F5 VIP)からDNS応答が送信されることを期待していましたが、異なるIPアドレス（バックエンドサーバー）から応答を受信していたため、DNS解決に失敗しました。

関連コンテンツ

- F5 GTMロードバランシングの設定
- シスコのテクニカルサポートとダウンロード

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。