セキュアアクセスWebセキュリティが有効な状態でのAzure VPNクライアント接続の失敗

内容

お問い合わせ内容

UmbrellaからSSEに移行し、新しく割り当てられたSIAライセンスでWebセキュリティを有効にすると、Webセキュリティが有効な場合にAzure VPN Client接続をユーザーに対して確立できなくなります。Azure VPNクライアントの接続の問題は、すべてのクライアントに影響を与え、VPNへの接続を妨げます。Cisco Secure Access Clientがクライアントマシンからアンインストールされると、VPN接続が復元されます。これは、Secure Access ClientがAzure VPNサービスへの接続をブロックしていることを示します。

Webセキュリティを無効にするか、Cisco Secure Access Clientをアンインストールすると、VPN接続が復元されますが、Webセキュリティ保護が必要な場合にAzure VPNを介したリソースへのユーザーアクセスに影響します。

環境

- Webセキュリティを有効にしたCisco Secure Access（以前のSIA）
- Azure VPNクライアント
- UmbrellaからSSEへの移行が完了
- 新しく割り当てられたSIAライセンス

解決策

この問題を解決するには、Azure VPNゲートウェイのパブリックアドレスを SSE/SWG例外リストに追加して、VPN接続をブロックするトラフィックの傍受を防止する必要があります。

手順1: Azure VPN GatewayのIPアドレスを特定する

Azure VPNゲートウェイのパブリックIPアドレスを決定します。

ステップ2:SSE/SWGへのIPベースの例外の追加

1.- Azure Virtual GatewayパブリックIPアドレスをCisco Secure Access環境のSSE/SWG例外リストに追加します。

2.- Cisco Secure Access Dashboardにログインします – Connect - End user Connectivity - Internet Security - Add exceptionの順にクリックします。これにより、Secure Web GatewayがAzure VPNゲートウェイ宛てのトラフィックを傍受して検査することを防ぎます。

ステップ3:VPN接続をテストする

IPベースの例外を適用した後、Azure VPN接続をテストして、クライアントがWebセキュリティを有効にしてVPN接続を正常に確立できることを確認します。

ステップ4：テストの拡張

解決の完了を検討する前に、IPベースの例外のテストを環境全体の追加ユーザにまで拡張し、一貫した機能を確保します。

原因

この問題は、Secure Web Gateway(SWG)の例外メカニズムで、ドメインからIPへのキャッシュエントリを作成するためにドメインのDNSルックアップが必要であるために発生します。Azure VPNクライアントがVPN URLに対してDNSクエリを実行せずにIPアドレスに直接接続すると、SWGモジュールはドメインをIPアドレスにマップできません。その結果、SWGはIPアドレスへのトラフィックの検査と代行受信を継続し、VPN接続の確立を阻止します。

パケットキャプチャ分析では、VPN URLに対するDNSクエリも、AzureゲートウェイIPに対する可視のSWG代行受信トラフィックも示されませんでした。キャッシュ内に適切なドメインとIPのマッピングがないため、SWGが接続をブロックしていたことが確認されました。

関連コンテンツ

- 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。