Secure Access Microsoft 365のバイパス動作機能の互換性の確認

内容

問題

Microsoft 365互換性機能を有効にしてCisco Secure Accessを設定する場合、特定のMicrosoft関連の完全修飾ドメイン名(FQDN)がSecure Web Gateway(SWG)の処理やTLSの復号化から自動的にバイパスされるかどうかが不確実です。特に、次のドメインのバイパス動作について詳しく説明する必要があります。

- do.dsp.mp.mi crosoft.com
- dl.delivery.mp.mi crosoft.com
- manage.microsoft.com

主な懸念事項は、これらのドメインがDo Not Decryptリストに手動で追加する必要があるかどうか、またはMicrosoft 365互換性が有効なときに自動的に除外されるかどうかです。また、SWGレベルのバイパスとIPSレベルの復号化設定とのインタラクションに関する混乱が見られます。特に、マニュアルに記載されているmanage.microsoft.comでは、Do Not Decrypt Listを手動で設定する必要がまだあることを示唆しています。

環境

- シスコセキュアアクセス
- Microsoft 365互換機能が有効
- Secure Web Gateway(SWG)インスペクションおよびTLS復号化の設定
- 使用中のIPS復号化ポリシー
- 接続を必要とするMicrosoft管理および更新サービス

解決方法

Microsoft 365互換性機能の動作は、次の結果を伴うラボテストによって検証されました。

Microsoft 365互換機能の範囲

Microsoft 365互換機能により、Microsoftのエンドポイントカテゴリで「Optimize」および「Allow」とマークされたMicrosoft 365関連ドメインは、SWGインスペクションおよびポリシー適用から除外されます。これにより、これらのドメインへのトラフィックは、SWGレイヤで変更されずに通過できます。

ラボテストの結果

テストは、Microsoft 365互換が有効になっている管理されたラボ環境で実施されました。この動作は、指定されたFQDNで確認されました：

ステップ1: Microsoft 365互換機能を有効にする

Microsoft 365互換機能がセキュアアクセス設定でアクティブになりました。

手順2：ターゲットFQDNへのトラフィックをテストする

Webトラフィックは、標準のインターネットブラウザを使用して、3つのFQDNのそれぞれに対して生成されました。

- do.dsp.mp.mi crosoft.com
- dl.delivery.mp.mi crosoft.com
- manage.microsoft.com

手順3：ダッシュボードでバイパス動作を確認する

セキュアアクセスダッシュボードの分析により、Microsoft 365互換機能が有効になっている場合

、これらの特定の宛先へのトラフィックに対してWebトラフィックの検査と復号化が行われていないことが確認されました。

ステップ4: DNSステアリング動作の確認

これらの宛先へのDNSトラフィックは引き続きセキュアアクセスを介して転送され、特定のDNS除外が設定されていない限り、ドキュメントに記載された動作に対応します。

主な動作調査結果

テスト結果とドキュメント分析に基づく：

- SWGバイパス：Microsoft 365互換が有効な場合、指定された3つのFQDNはWebトラフィック検査からバイパスされます。
- TLS復号化：これらのドメインのSWGレイヤで復号化がバイパスされます。
- DNSステアリング：DNSクエリは、明示的に除外されない限り、引き続きセキュアアクセスを介して処理されます。
- ドメインカバレッジ：ドメイン全体としての「*.microsoft.com」は仕様によって完全にバイパスされませんが、実際にはテストされる特定のURLはバイパスされます。

IPSレイヤの考慮事項

Microsoft 365互換機能はSWGレイヤで動作します。IPSレベルの復号化バイパスの場合でも、次のように手動で設定する必要があります。

- これらのドメインでIPS復号化バイパスも必要な場合は、Do Not Decryptリストに手動で追加する必要があります。
- Do Not Decrypt Listは、主にSWG処理ではなくIPS側の復号化に影響を与えます。
- Microsoft 365の互換性が有効な場合でも、ドキュメントで「Do Not Decrypt List」へのmanage.microsoft.comの追加を参照できる理由は、次のとおりです。

原因

混乱の原因は、Cisco Secure Accessの階層型アーキテクチャにあります。このアーキテクチャでは、Microsoft 365の互換性がSWGレベルの処理に影響を与えますが、IPSの復号化は独自の設定要件を持つ別のレイヤとして動作します。Microsoft 365互換機能は、正規のMicrosoftドメインに対するSWGバイパスを自動的に処理しますが、IPS復号化ポリシーでは、Do Not Decrypt Listを使用して個別に設定する必要がある場合があります。

関連コンテンツ

- Cisco Secure Access Microsoft 365互換性に関するドキュメント
- Cisco Secure Access用の有効なDo Not Decryptリストの作成
- 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。