

Meraki統合によるセキュアアクセスを介したAzureでホストされたFQDN接続の問題

内容

お問い合わせ内容

セキュリティアクセスログでトラフィックが「許可」と表示されているにもかかわらず、ユーザーがトラフィックがMeraki経由でCisco Secure Accessにルーティングされると、特定のAzureでホストされたFQDNに到達できなくなります。この問題は、これらのFQDNへの非標準ポートを使用するRDP接続に主に影響します。

セキュアアクセスポータルでFQDNでログを検索すると、DNSセキュリティログのみが表示され、「許可」ステータスが示されます。ただし、非標準ポート上の同じ宛先へのRDP接続は失敗します。FQDNがIPアドレスに解決され、アクティビティ検索が宛先IPを使用すると、トラフィックをブロックしていたクラウドファイアウォールのログが表示されます。

環境

- Cisco Secure Access(SSE)とMerakiの統合
- ローカルブレイクアウト機能を備えたMerakiダッシュボード
- 非標準ポートでのRDPアクセスを必要とする、Azureでホストされた開発リソース
- セキュアアクセスへのMerakiトンネルを介したトラフィックルーティング

解決策

当面の回避策

次のセクションで詳しく説明するように、影響を受けるFQDNをMerakiローカルブレイクアウトルールに追加して、特定の宛先に対するセキュアアクセスをバイパスします。

ステップ1:Merakiダッシュボードへのアクセス

Merakiダッシュボードに移動し、ローカルブレイクアウト設定セクションを見つけます。

ステップ2：ローカルブレイクアウトルールの設定

問題のあるFQDNをローカルブレイクアウトルールに追加して、セキュアアクセスルーティングをバイパスします。この設定変更により、Merakiからインターネットに直接トラフィックがルーティングされ、セキュアアクセストンネルがバイパスされるため、影響を受けるユーザのアクセスが即座に回復されます。

トラブルシューティングと分析

ステップ1:FQDNによるログ分析

FQDNを使用して、セキュアアクセスアクティビティ(PAC)ログを検索します。これは主にDNSセキュリティログを示し、ポート443のWebトラフィックの「allowed」ステータスを表示できます。

ステップ2：宛先IPによるログ分析

FQDNをIPアドレスに解決し、FQDNの代わりに宛先IPを使用してアクティビティログを検索します。これにより、ブロックされたトラフィックを示すクラウドファイアウォールのログが明らかになり、実際のトラフィックの性質がわかります。

手順3：トラフィックフローの確認

この問題が発生するのは、トラフィックがパス「User → Meraki → Tunnel → Secure Access → Internet」をたどる場合だけであることを確認します。ローカルブレイクアウトを介してバイパスするテストによって、接続の問題が解決されます。

長期的な解決策

確認された動作は、現在のセキュアアクセス実装で期待される機能として特定されています。機能リクエスト(FR CSE-I-5543)が開始され、以下に関連する可視性と機能の問題に対処します。

- FQDNベースのログ検索とIPベースのログ検索の不一致
- DNSセキュリティとクラウドファイアウォールのログ間の一貫性のないトラフィック破棄レポート
- 非標準ポート上のRDPトラフィックの可視性の向上

原因

この問題は、Secure Accessが非標準ポートでRDPを介してアクセスされた際に、AzureがホストするFQDNのトラフィックを処理および報告する方法に不一致があることに起因します。

FQDNでログを検索すると、主にDNSセキュリティログが表示され、Webトラフィックの「許可」ステータス(通常はポート443)が示されます。ただし、非標準ポート上の実際のRDPトラフィックは、クラウドファイアウォールルールによって処理されています。このルールは、FQDNではなく解決済みの宛先IPアドレスで検索した場合にのみ表示されます。

これにより、管理者はFQDNベースの検索で「許可された」トラフィックを確認する一方で、実際のRDP接続は、IPベースのログ検索でのみ明らかになるファイアウォールポリシーによってブロックされる可視性のギャップが生じます。この動作は現在期待される機能と見なされていますが、さまざまな検索方法のトラフィックレポートの可視性と一貫性を向上させるための機能要求が送信されています。

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。