セキュアアクセス：アイドルタイムアウトエラーにより、企業ファイアウォールの背後で断続的に切断

内容

- お問い合わせ内容
- 環境
- 解決策
  - ステップ1:MX TTLバッファ設定の実装
  - ステップ2：必要なドメイン除外を設定する
  - ステップ3：ポートおよびプロトコルの許容範囲の確認
  - ステップ4：解決の監視と検証
- 原因
- 関連コンテンツ

お問い合わせ内容

Cisco Secure Accessクライアントでは、エンドポイントが企業ネットワークに接続されると、接続が断続的に解除され、すぐに再接続されます。接続がランダムに解除され、約5秒後にクライアントが自動的に再接続されます。この動作は、ゼロトラストアクセス(ZTA)を介してインターネットトラフィックをプロキシし、Cisco FirePowerおよびMeraki MXデバイスの背後に配置されたエンドポイントからのアクセスを保護する場合に発生します。

Windowsのイベントログには、これらの切断イベント中の特定の「idleTimeout」エラーが記録されます。ユーザがホームインターネット接続から接続する場合は切断パターンは発生せず、問題が特に企業ネットワークインフラストラクチャに関連していることを示します。

この症状により、企業のネットワーク環境内で稼働するユーザのリモートアクセス接続を保護するというビジネス中断が発生しますが、リモートユーザはこの接続上の問題には該当しません。

環境

- Cisco Secure Access – アドバンテージの導入
- Cisco Secure Internet Access(SIA)クライアントソフトウェア
- Cisco FirePowerセキュリティアプライアンスを使用した企業ネットワークインフラストラクチャ
- ネットワークパス内のMeraki MXセキュリティアプライアンス
- ゼロトラストアクセス(ZTA)設定によるインターネットトラフィックのセキュアアクセスへのプロキシ
- イベントロギング機能を備えたWindowsエンドポイント
- 混合接続シナリオ：企業ネットワーク（該当）とホームインターネット接続（該当なし）

解決策

この問題を解決するには、Meraki MXデバイスの設定変更を実施し、Secure Access統合のための適切なドメイン除外とポート許可を確保する必要がありました。

ステップ1:MX TTLバッファ設定の実装

Meraki MXデバイスでMX TTLバッファを設定し、断続的な接続解除問題の原因となっていたDNS TTLキャッシュ動作に対処します。この設定変更により、DNS解決キャッシングとセキュアアクセスクライアントの接続の期待値との間のタイミングの競合が解決されます。

ステップ2：必要なドメイン除外を設定する

次のドメインが傍受から適切に除外され、Cisco FirePowerとMeraki MXの両方のデバイスの非復号化リストに追加されていることを確認します。

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- ポリシー設定で特定された追加のSecure Accessサービスドメイン

ステップ3：ポートおよびプロトコルの許容範囲の確認

FirePowerとMeraki MXの両方のデバイスを介して必要なセキュアアクセスポートとプロトコルを許可するように、企業のファイアウォールインフラストラクチャを設定します。Secure Accessサービスエンドポイントのポート443へのトラフィックが、タイムアウト状態を引き起こす可能性があるセキュリティ検査の干渉なしで適切に処理されていることを確認します。

ステップ4：解決の監視と検証

MX TTLバッファ設定を実装した後、Secure Accessクライアントの動作を数日間監視して、断続的な接続解除と再接続のパターンが停止したことを確認します。

原因

断続的な切断は、企業ネットワークインフラストラクチャとSecure Accessサービスの期待値との間でDNS TTL（存続可能時間）キャッシング動作の競合が発生したことが原因です。シスコの技術分析により、DNSのTTL値はリゾルバのキャッシング動作によって異なり、IPアドレスの交互交換はSecure Accessサービスアーキテクチャのロードバランシングメカニズムによって予期される動作であることが判明しました。

企業のネットワークデバイス（Cisco FirePowerおよびMeraki MX）がセキュアアクセスエンドポイントのDNS応答を処理すると、キャッシングとTTL処理によってタイミングの不一致が生じ、「idleTimeout」状態が発生しました。このタイミングの競合により、Secure Accessクライアントは接続をアイドルとして解釈し、接続解除/再接続サイクルを開始しました。

この問題は、企業ネットワーク環境に固有のものです。これは、一般的に、ホームインターネッ

ト接続では、セキュアアクセスクライアントの接続状態管理を妨げる可能性があるDNSキャッシングとトラフィック検査のレベルが実装されていないためです。

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。