macOSのハイバネーション後のクライアントZTNA DNS解決と接続の損失の保護

内容

お問い合わせ内容

macOSエンドポイント上のCisco SecureClient ZTNAで、システムがスリープまたは休止モードから再開した後、DNS解決の失敗とZTA接続の喪失が発生します。この問題は、ZTNA IA（アイデンティティアクセス）とZTNA PA（プライベートアクセス）の両方の機能に影響します。基本的なIP接続は引き続き機能しますが（8.8.8.8や208.67.222.222などの外部IPアドレスに対するICMP pingは正常に機能します）、DNS名前解決は完全に失敗し、インターネットリソースとZTNAを通じて設定されたプライベートリソースの両方へのアクセスができなくなります。

確認された具体的な症状は次のとおりです。

- nslookupコマンドを使用したDNSルックアップが失敗する（8.8.8.8経由のwww.cisco.comのnslookupと同様、208.67.222.222は機能しない）。
- ZTNA IAおよびZTNA PA接続が使用できなくなります。
- 問題は、エンドポイントの休止サイクルとウェイクアップサイクルの後に一貫して発生します。
- また、デバイスがアクティブに使用されている間にランダムに発生する可能性もあります。
- ZTNAプロセスを強制終了すると即座に再起動しますが、通常は接続の問題が解決されません。
- 完全なシステムリブートのみが、完全なDNS解決とZTNA接続を復元します。

環境

- オペレーティングシステム：macOS（バージョン26.3のケースに記載）
- Cisco SecureClient：バージョン5.1.14.x（影響を受ける5.1.16より前のバージョン）

- ZTNAモジュール：アイデンティティアクセス(IA)とプライベートアクセス(PA)の両方の設定でアクティブ
- ネットワークモニタリング：Sentinel Oneなどのサードパーティのセキュリティソリューションを含めることができます。
- 追加のセキュリティソフトウェア：Cisco Secure Endpointを含めることができます。
- DNSサーバ：外部DNSサーバ(8.8.8.8、208.67.222.222)にICMP経由でアクセスできるが、DNS解決が失敗する
- UMBモジュール：使用されていません

解決策

この問題は、シスコのエンジニアリング部門から提供されたソフトウェア修正で解決されました。解決プロセスには、次のセクションで説明する手順が含まれます。

ステップ1：問題の特定とバグトラッキング

シスコのエンジニアリング部門では、これを既知の不具合として特定し、Cisco Bug ID CSCwt24392に「macOS: DNS stops working with ZTA SIA-all and NVM active」という説明を付けて記録しました。

ステップ2：診断データの収集

この診断情報は、エンジニアリング分析をサポートするために収集されました。

- 該当するエンドポイントからのDART（診断およびレポートツール）バンドル。
- パケットキャプチャファイル(ZTNA Issue1.pcapng)。
- 接続障害を示すスクリーンショット
- 問題の再現を示す画面レコーディング
- com.cisco.secureclient.zta.app.serviceとシステム拡張プロセスの動作を示すプロセス対話ロ

グ。

ステップ3：エンジニアリング修正プログラムの開発

シスコのエンジニアリング部門では、CSCwt24392のターゲットを絞った修正を開発し、SecureClientリリースバージョン5.1.16に含めました。この修正は、スリープ/休止サイクル後にZTA SIA-allおよびNVMがmacOSシステムでアクティブになったときに発生するDNS解決障害に特に対処するものです。

ステップ4：ソフトウェア更新プログラムのインストール

該当するmacOSエンドポイントに、Cisco SecureClientバージョン5.1.16以降をインストールします。このバージョンには、DNS解決とZTA接続の問題に対する修正が含まれています。

ステップ5：検証テスト

SecureClient 5.1.16をインストールした後、次の検証手順を実行します。

1.- macOSエンドポイントがスリープまたは休止モードに入ることを許可します。

2. – システムをスリープまたは休止状態から解除します。

3.- nslookupコマンドを使用してDNS解決をテストします。

4. – 構成されたリソースへのZTNA IAおよびZTNA PAの接続を確認します。

5. – システムを再起動せずに、インターネットアクセスとプライベートリソースアクセスの両方が正しく機能することを確認します。

以前のバージョンでの回避策

SecureClient 5.1.16への即時アップグレードが不可能な環境では、次の一時的な回避策を使用できます。

- スリープ/休止サイクルごとにシステム全体を再起動して、DNS解決とZTNA接続を復元します。
- スリープ/休止の問題が生産性に大きな影響を与える場合は、ZTNAから一時的に登録解除することを検討してください（これにより、ZTNA保護が削除されることに注意してください）。

原因

この問題の根本的な原因は、5.1.16より前のCisco SecureClientバージョンのソフトウェア不具合で、Cisco Bug ID CSCwt24392として特に追跡されています。この不具合は、ZTA(Zero Trust Access)のSIA-all(Secure Internet Access)コンポーネントとNVM(Network Visibility Module)コンポーネントがmacOSシステムでアクティブになっている場合に発生します。スリープまたは休止状態およびスリープ解除サイクルの間、これらのコンポーネントは、基本的なIP接続を維持しながら、DNS解決機能を適切に復元できません。これにより、ICMPトラフィック(ping)は正常に機能するが、DNSクエリは失敗し、インターネットリソースおよびZTNAで保護されたプライベートリソースへのアクセスが実質的にブロックされる状態が生じます。この問題は、システム状態の移行中におけるcom.cisco.secureclient.zta.app.serviceプロセスとシステム拡張プロセスの間の不適切なインタラクションに関連しています。

関連コンテンツ

- Cisco Bug ID CSCwt24392 - macOS:ZTA SIA-allおよびNVMがアクティブの状態でDNSの動作が停止する
- 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。