

CodexアプリケーションのDNSストームが原因で、セキュアクライアントUmbrellaモジュールが非アクティブになる

内容

問題

MacOSの複数のユーザで、Cisco Secure Client Umbrellaローミングモジュールが断続的に非アクティブ（フェールオープン）状態に移行することがあります。この間、ターミナルから開始されるnslookupコマンドなどのDNS要求はネットワーク層に到達しないため、ドメインを解決するユーザやインターネットベースのリソースにアクセスするユーザの機能に影響を与えます。

この問題は、Umbrellaログでプローブ障害が繰り返し発生し、次のようなメッセージが表示される場合に発生します。

```
Transparent probe failed
Encrypted probe failed
Switching to basic probe
DNS probe failed by timeout - going open
```

分析の結果、Umbrellaが非アクティブになると、同じ障害ウィンドウ中にコンソールドライバがクラッシュすることが判明しました。この問題は、ユーザがCodexおよびAI Assistantアプリケーションをアクティブに使用しているときに最も頻繁に発生し、CODEXにコマンドが送信された直後にchatgpt.comへの大量の接続が試行されます。

環境

- Cisco Secure Client/バージョン5.1.13、5.1.16、5.1.17
- macOS（複数のバージョンを確認）
- Umbrellaローミングモジュールが有効

- ZTNA/セキュアインターネットアクセス(SIA)モジュールが有効
- 使用中のCodexアプリケーション
- さまざまなネットワーク (自宅、オフィス、さまざまなISP) で働くユーザー

解決方法

この問題は、ドメインバイパス設定を実装してDNS要求の重複を防止することで解決されました。次のセクションで説明するアプローチが検証されました。

主な解決策：ドメインのバイパス

- ステップ1: Cisco Secure Access設定のバイパスリストにchatgpt.comを追加します。これにより、セキュアクライアントはCodexアプリケーションによって生成されたDNS要求を複製できなくなり、ドライバの不安定性を引き起こすDNSストームが解消されます。
- ステップ2：バイパス設定を確認します。Codex機能をテストして、バイパスが設定された状態で問題が再発しなくなったことを確認します。

代替解決策：Codex設定の回避策

GitHub問題で参照されているCodex構成の変更を適用し、アプリケーションによって生成されるDNS要求のボリュームを減らします。 <https://github.com/openai/codex/issues/21218>

使用される高度なトラブルシューティング手順

これらの診断手順は、根本原因を特定するために実行されました。

1. – 詳細なコンソールロギングを有効にします。

```
sudo /opt/cisco/secureclient/kdf/bin/acsocketool -sdf 0x830801F2
```

2. – 問題を再現し、障害の直後にDARTバンドルを収集します。

3. – 詳細ロギングを無効にします。

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4.- SWGの最大デバッグロギングを有効にします。コンテンツを含むSWGConfigOverride.jsonファイルを作成します。

```
{"logLevel": "1"}
```

/opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.jsonに保存します。

5.- DNSのRSMトレースログを有効にします。force_log_level.plistファイルをコンテンツとともに作成します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

/opt/cisco/secureclient/umbrella/dataに保存します。

原因

主な問題は、大量のDNS要求を生成するCodexアプリケーションの動作に関連しています。chatgpt.comがバイパスされないと、これらの要求はCisco Secure Clientによって実質的に複製され、DNSストームが発生してCPU使用率が高くなり、カーネルドライバが不安定になります。

この問題は、次の理由で発生します。

- Codexは、動作中にchatgpt.comに対して多数のDNSクエリを生成します。
- バイパス設定を行わないと、セキュアクライアントはこれらの要求を代行受信して複製します。
- 重複した大量のDNS要求により、acsockドライバがクラッシュします。
- ドライバが不安定になると、Umbrellaプロンプトが失敗し、フェールオープン状態に移行します。

chatgpt.comをバイパスするか、Codexの回避策を適用すると、この重複は発生せず、問題が再発しなくなります。この問題は、Umbrella専用とZTNA SIAの両方の設定に影響を与え、問題が特定のモジュールではなくトラフィック処理メカニズムにあることを示します。

関連コンテンツ

- [セキュアアクセスローミングモジュールのトラブルシューティング](#)
- [トラブルシューティングと基本情報の収集](#)
- [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。

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。