セキュアアクセスローミングモジュール"；クラウドサービス使用不可"；または"；保護されていない"；ステータスのトラブルシューティング

内容

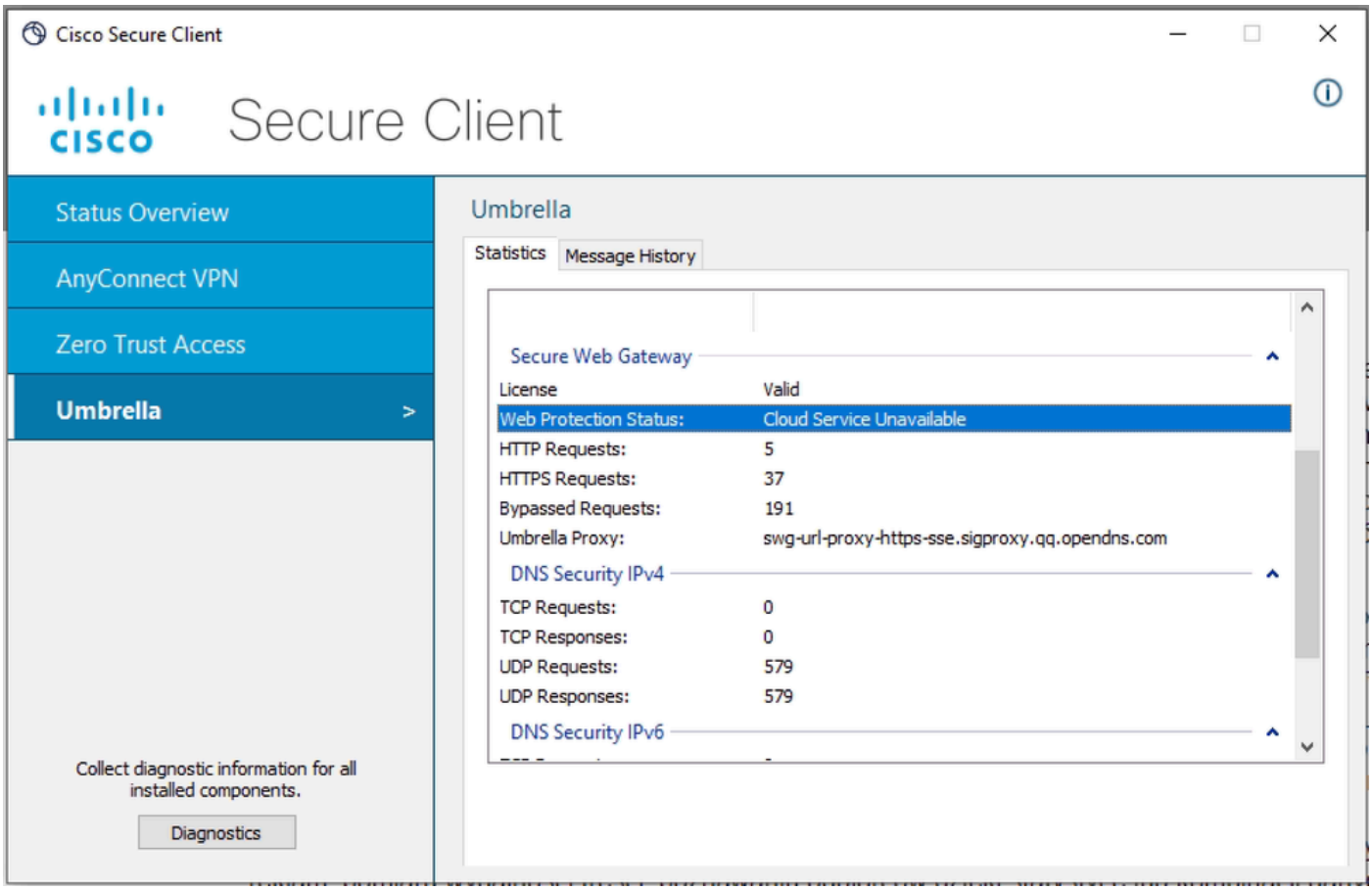
はじめに

このドキュメントでは、セキュアクライアントのRoamingモジュールのステータス「Cloud Service Unavailable」または「Unprotected」の根本原因を調査する方法について説明します。

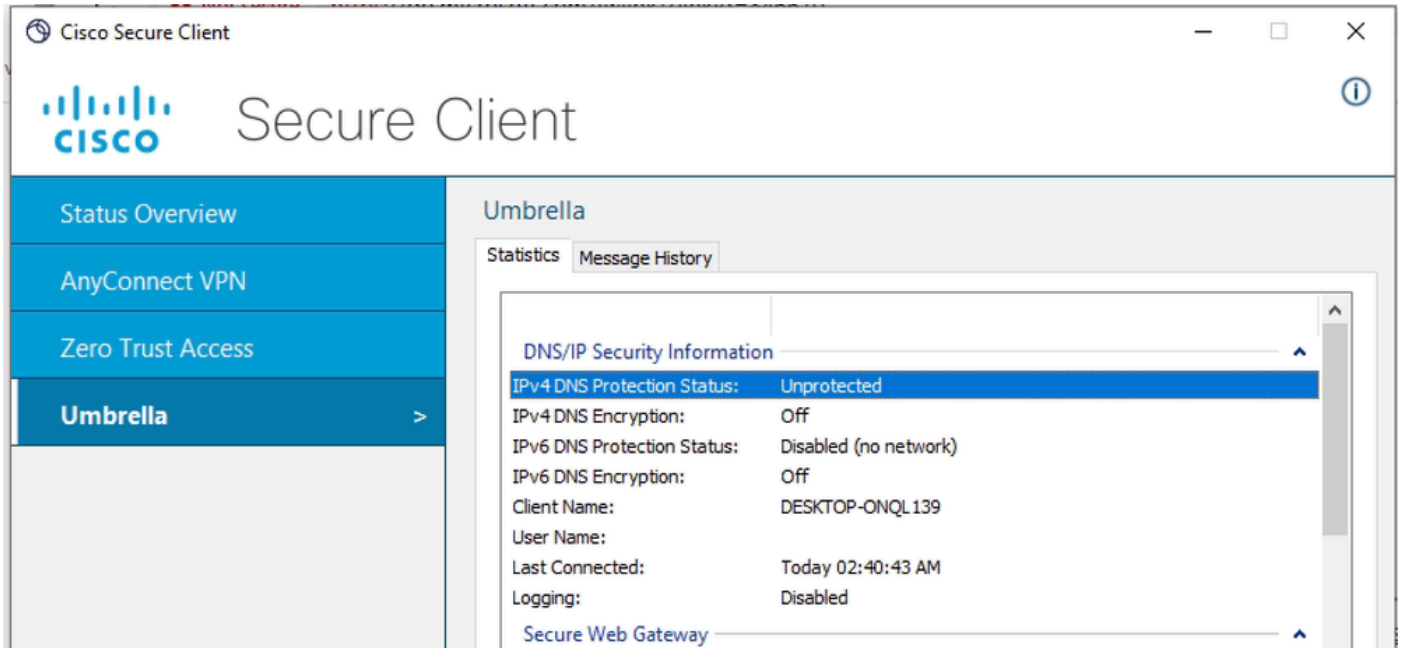
問題

ユーザがセキュアクライアントのRoamingモジュールを起動し、DNSやWeb保護の使用を予定している場合、セキュアクライアントユーザインターフェイスに誤った状態が表示される可能性があります。

Web保護の状態に対してクラウドサービスを使用できません



DNS保護ステータスの保護なし



これらのエラーの原因は、ネットワーク接続の問題が原因でRoaming Moduleがクラウドサービスに接続できないことです。

この問題が該当するクライアントPCで過去に発生していない場合は、PCが接続されているほとんどのネットワークが制限されており、「SSEドキュメント」に概説されている要件を満たしていないことを意味しています。

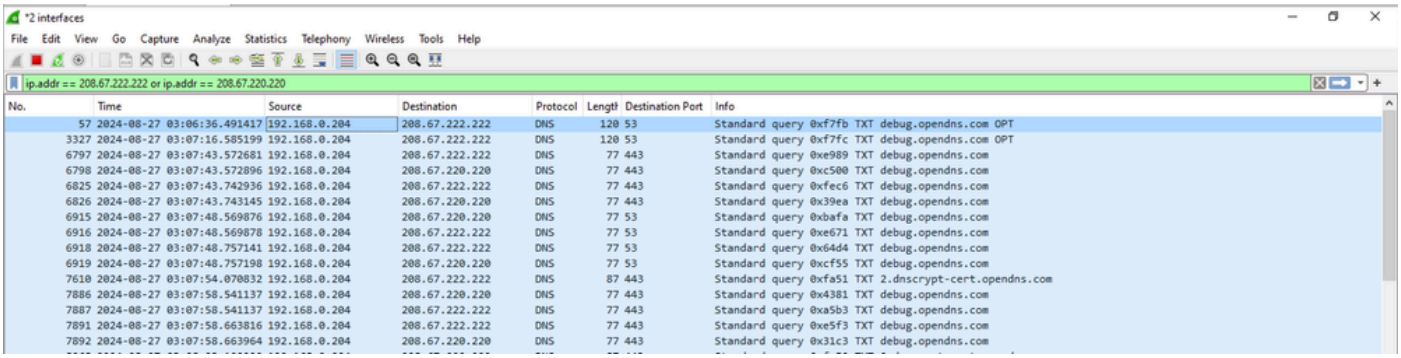
DNS保護の状態が保護されていません

Unprotected DNS状態が表示される場合、最も可能性の高い原因として、Roaming Module(ROAMING)からOpenDNSサーバへのアップストリーム接続が存在していないことが考えられます(208.67.222.222および208.67.220.220)。
ログは、DARTバンドルの一部であるcscumbrellaplugin.txtファイルに記録されています。

```
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:43 [8880] [DEBUG] < 13> Dns Protection IPv6 State Machine: rejected all candidate reso
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:53 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: rejected all candidate reso
```

接続の問題のダブルチェックと確認を行うには、PCの出力物理インターフェイス（WiFiまたはイーサネット）でWiresharkキャプチャを収集し、表示フィルタを使用してOpenDNSリゾルバを宛先とするトラフィックのみを検索できます。

```
ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220
```



Wiresharkからのスニペットで示されているように、クライアントがUDPポート443および53で208.67.222.222および208.67.220.220宛てのDNS TXTクエリを再送信し続けるものの、応答を受信していないことは明らかです。

このような動作には、複数の原因が考えられます。最も可能性が高いのは、境界ファイアウォールデバイスがOpenDNSサーバへの出力DNSトラフィックをブロックしている、または特定のDNSサーバへのトラフィックのみを許可している場合です。

Web保護の状態がクラウドサービスを利用できません

「Service Unavailable Web protection」状態が表示された場合、最も可能性の高い方法は、Roaming ModuleからSecure Web Gatewayサーバへのアップストリーム接続が存在しないことです。

PCからSWGサーバにIP接続できない場合は、DARTバンドルの一部であるUmbrella.txtファイルにログが記録されています。

```
Date : 08/27/2024
Time : 06:41:22
Type : Warning
Source : csc_swgagent

Description : WARN | Thread 27cc | TCP handshake to SWG Proxy URL was not successful. Since fail open p
```

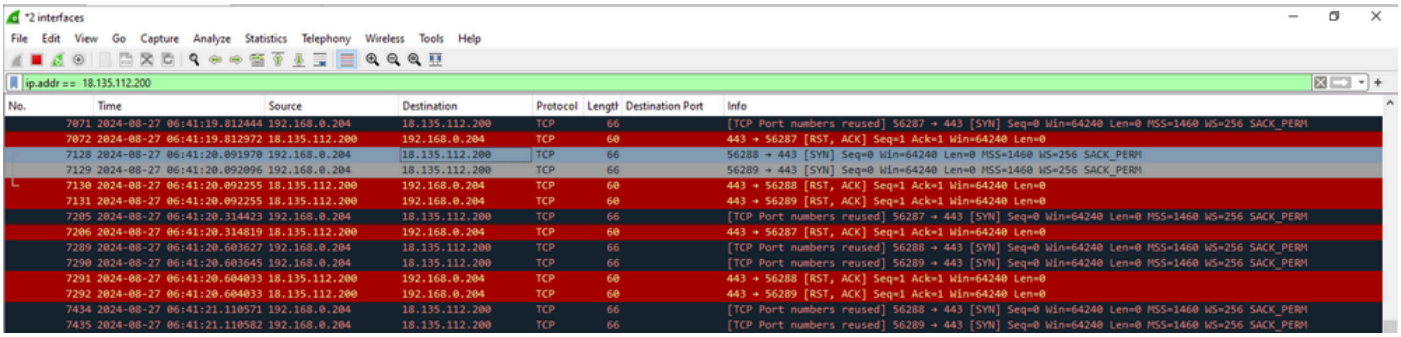
さらに調査するには、パケットキャプチャを収集して、PCがSWGサーバに接続されていないことを証明します。
端末でコマンドを発行して、SWGのIPアドレスを取得します。

<#root>

```
C:\Users\admin>

nslookup swg-url-proxy-https-sse.sigproxy.qq.opendns.com


Server: ad.lab.local
Address: 192.168.0.65

Non-authoritative answer:
Name: k8s-sigproxy-sigproxy-c8f482b42a-ddf1929ae349b3e5.elb.eu-west-2.amazonaws.com
Address:

18.135.112.200


Aliases: swg-url-proxy-https-sse.sigproxy.qq.opendns.com
swg-proxy_eu-west-2_1_1n.sigproxy.aws.umbrella.com
```

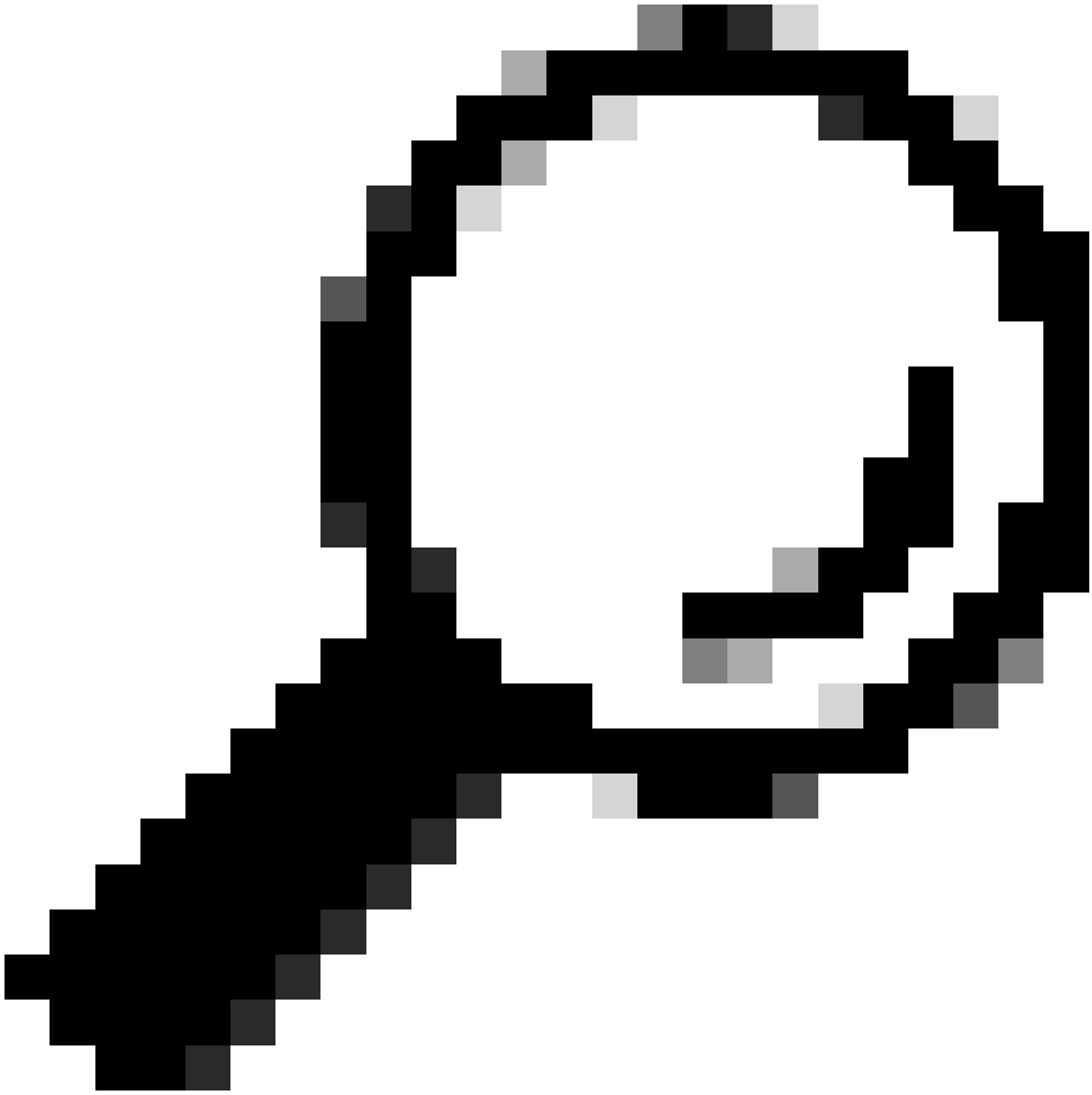
接続の問題の再確認と確認を行うために、PCの出力物理インターフェイス（WiFiまたはイーサネット）でWiresharkキャプチャを収集し、表示フィルタを使用してSWGサーバ宛てのトラフィックのみを検索できます（前の手順で取得したIPアドレスを使用）

```
ip.addr == 18.135.112.200
```



Wiresharkからのスニペットでわかるように、クライアントが18.135.112.200を宛先とするTCP SYNパケットを再送信し続けるものの、応答としてTCP RSTを受信していることがわかります。

この特定のラボシナリオでは、境界ファイアウォールがSWG IPアドレスへのトラフィックをブロックしていました。
実際のシナリオでは、TCP SYNの再送信だけが確認でき、TCP RSTは確認できません。



ヒント：クライアントがSWGサーバに到達できない場合、デフォルトで、Webトラフィック（WebトラフィックはWiFiまたはイーサネット）が直接インターネットアクセス経由で発信されるfail open状態になります。フェールオープンモードでは、Web保護は適用されません。

解決方法

根本的なネットワークが問題を引き起こしていることを迅速に特定するために、ユーザは境界ファイアウォールを持たない他のオープンネットワーク（ホットストップ、ホームWi-Fi）に接続できます。

上記の接続エラーを修正するには、SSEドキュメントに記載されているように、PCに無制限のアップストリーム接続があることを確認してください。

DNS保護ステータスの問題：

- 208.67.222.222 TCP/UDPポート53
- 208.67.220.220 TCP/UDPポート53

Web保護ステータスの問題の場合は、入力IPアドレスへのトラフィックが境界ファイアウォールで許可されていることを確認します：SSEドキュメント

入力IPアドレスの具体的な範囲は、場所によって異なります。

関連情報

- セキュアアクセスユーザガイド
- Cisco Secure ClientからのDARTバンドルの収集方法
- テクニカル サポートとドキュメント - Cisco Systems

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。