

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](#)

[問題](#)

[DNS保護の状態が保護されていません](#)

[Web保護の状態がクラウドサービスを利用できません](#)

[解決方法](#)

[関連情報](#)

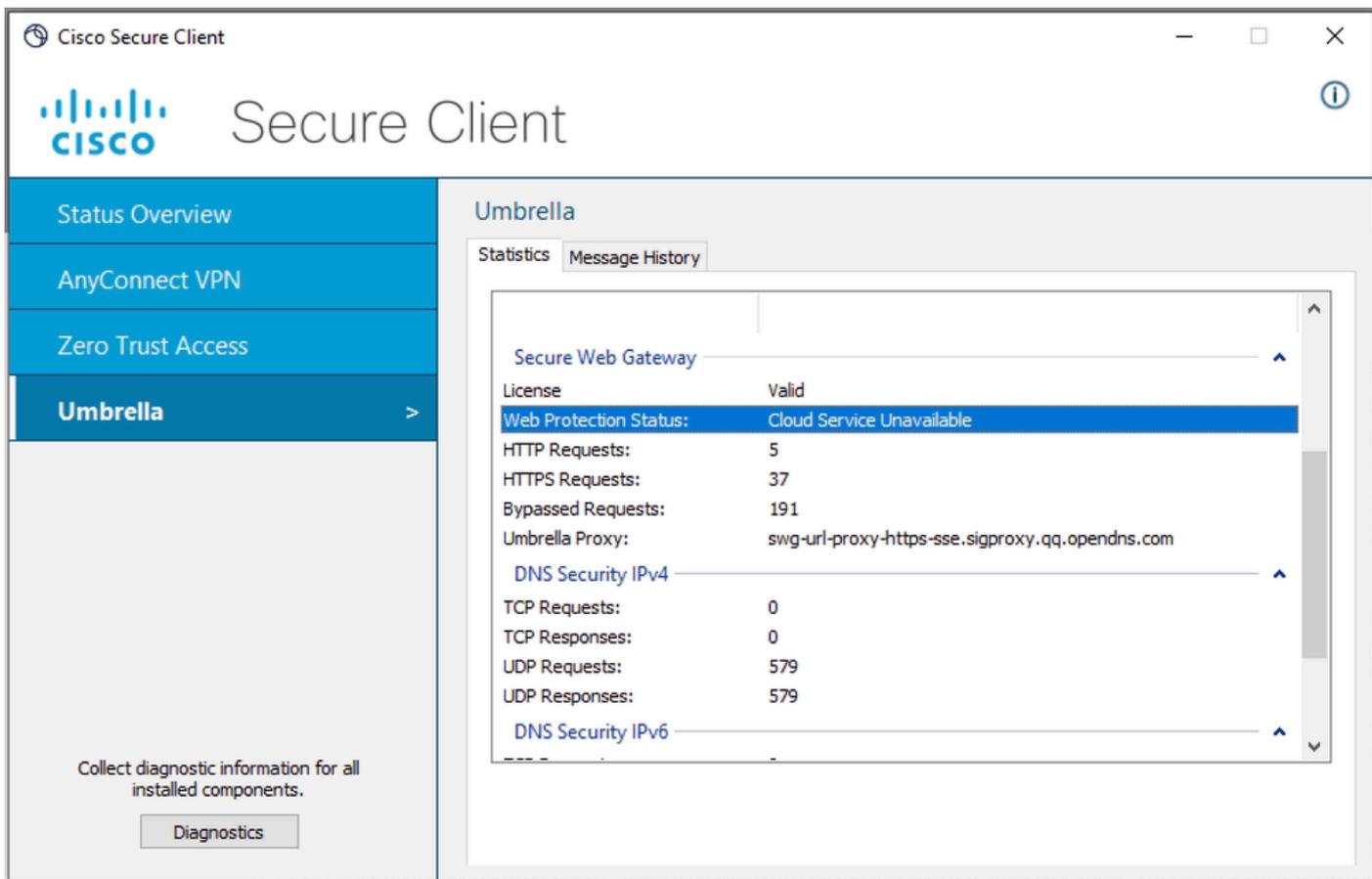
はじめに

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。

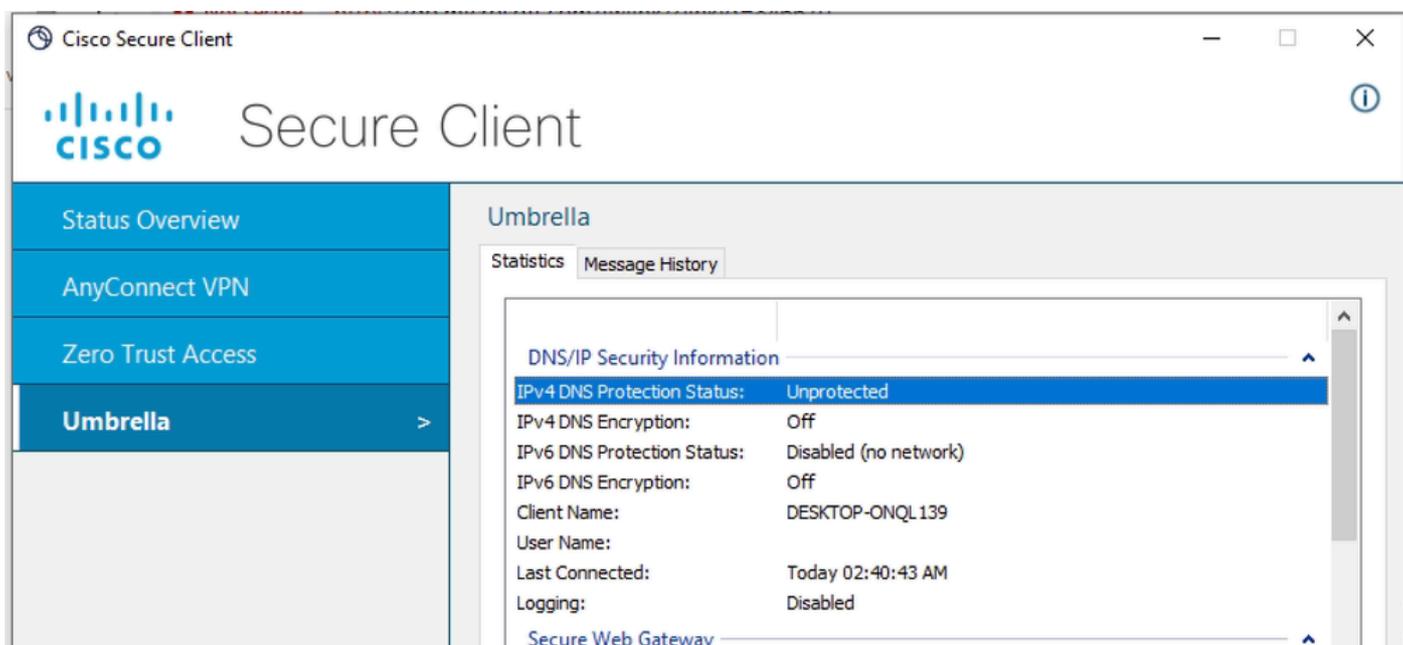
問題

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

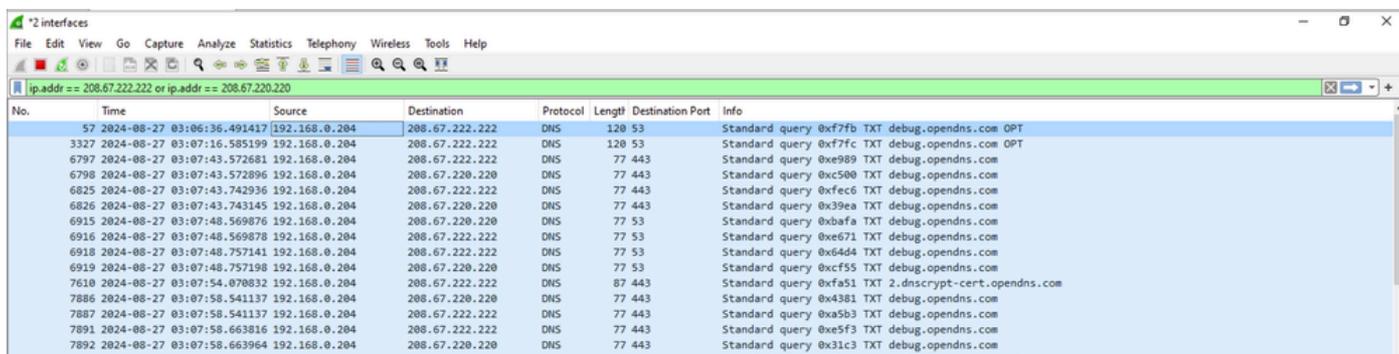
Unprotected DNS状態が表示される場合、最も可能性の高い原因として、Roaming Module(ROAMING)からOpenDNSサーバへのアップストリーム接続が存在していないことが考えられます(208.67.222.222および208.67.220.220)。

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
```



The image shows a Wireshark capture window with the filter 'ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220'. The capture shows a series of DNS queries from source IP 192.168.0.204 to destination IP 208.67.222.222 and 208.67.220.220. The queries are for TXT records from debug.opendns.com. The 'Info' column shows details like 'Standard query 0xf7fb TXT debug.opendns.com OPT'.

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
57	2024-08-27 03:06:36.491417	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fb TXT debug.opendns.com OPT
3327	2024-08-27 03:07:16.585199	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fc TXT debug.opendns.com OPT
6797	2024-08-27 03:07:43.572681	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe989 TXT debug.opendns.com
6798	2024-08-27 03:07:43.572896	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0xc500 TXT debug.opendns.com
6825	2024-08-27 03:07:43.742936	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xfec6 TXT debug.opendns.com
6826	2024-08-27 03:07:43.743145	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x39ea TXT debug.opendns.com
6915	2024-08-27 03:07:48.569876	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xbafa TXT debug.opendns.com
6916	2024-08-27 03:07:48.569878	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0xe671 TXT debug.opendns.com
6918	2024-08-27 03:07:48.757141	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0x64d4 TXT debug.opendns.com
6919	2024-08-27 03:07:48.757198	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xcf55 TXT debug.opendns.com
7610	2024-08-27 03:07:54.870832	192.168.0.204	208.67.222.222	DNS	87	443	Standard query 0xfa51 TXT 2.dnscrypt-cert.opendns.com
7886	2024-08-27 03:07:58.541137	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x43b1 TXT debug.opendns.com
7887	2024-08-27 03:07:58.541137	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xa5b3 TXT debug.opendns.com
7891	2024-08-27 03:07:58.663816	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe5f3 TXT debug.opendns.com
7892	2024-08-27 03:07:58.663964	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x31c3 TXT debug.opendns.com

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)

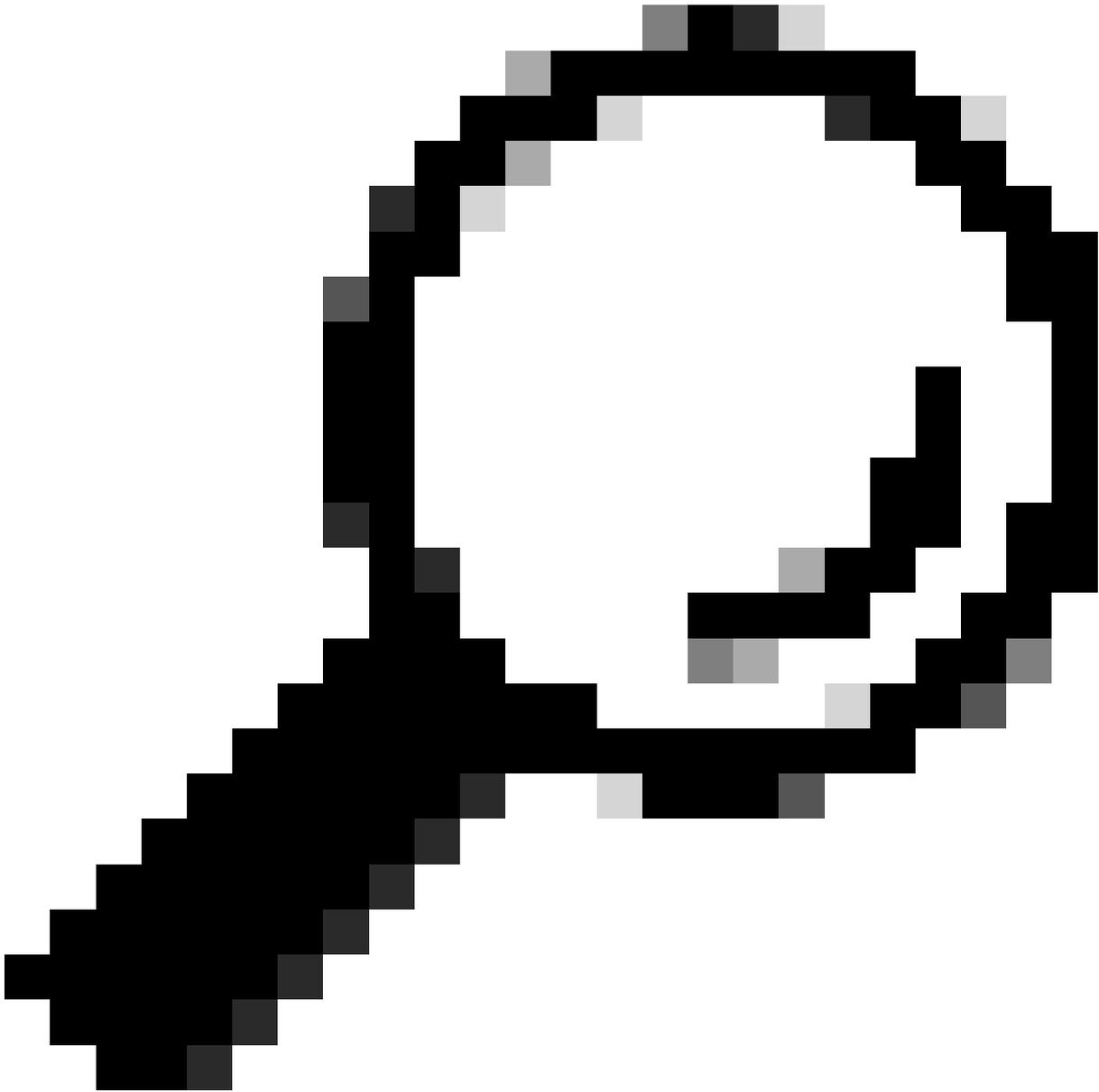
```
ip.addr == 18.135.112.200
```

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
7071	2024-08-27 06:41:19.812444	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7072	2024-08-27 06:41:19.812972	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7128	2024-08-27 06:41:20.091970	192.168.0.204	18.135.112.200	TCP	66		56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7129	2024-08-27 06:41:20.092096	192.168.0.204	18.135.112.200	TCP	66		56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7130	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7131	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7205	2024-08-27 06:41:20.314423	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7206	2024-08-27 06:41:20.314819	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7289	2024-08-27 06:41:20.603627	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7290	2024-08-27 06:41:20.603545	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7291	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7292	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7434	2024-08-27 06:41:21.110571	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7435	2024-08-27 06:41:21.110582	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

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（ホットスポット、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。