

# Secure Access Roaming Module "Cloud Service Unavailable" 또는 "Unprotected" 상태 문제 해결

## 목차

---

[소개](#)

[문제](#)

[DNS 보호 상태가 보호되지 않음](#)

[웹 보호 상태가 클라우드 서비스를 사용할 수 없음](#)

[솔루션](#)

[관련 정보](#)

---

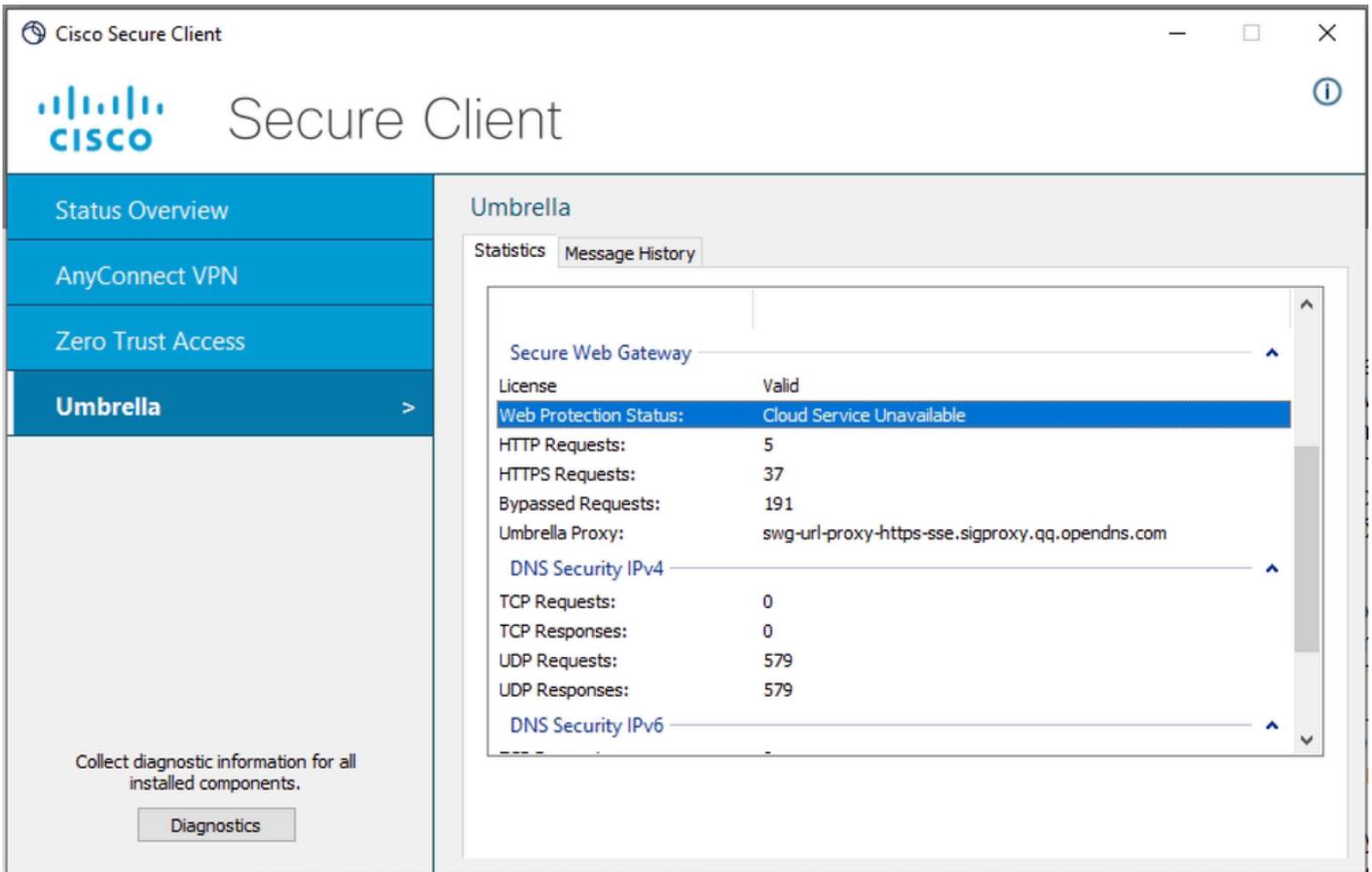
## 소개

이 문서에서는 Secure Client의 로밍 모듈에서 "클라우드 서비스를 사용할 수 없음" 또는 "보호되지 않음" 상태의 근본 원인을 조사하는 방법에 대해 설명합니다.

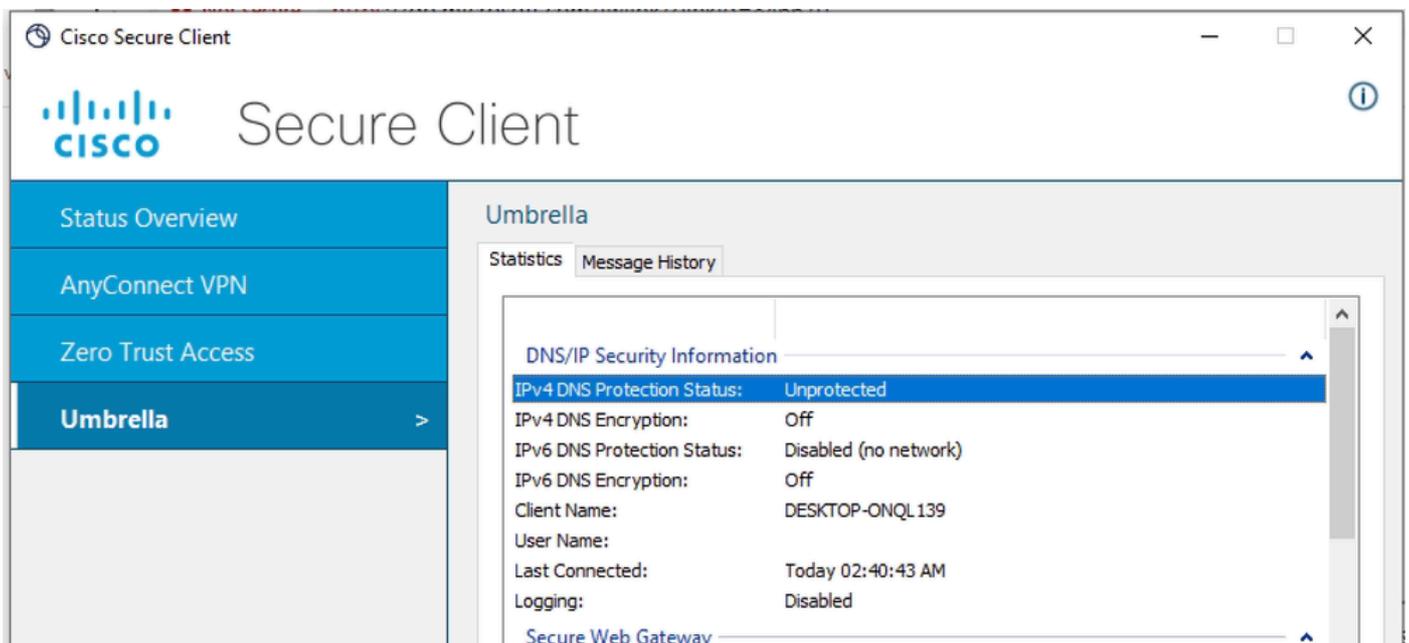
## 문제

사용자가 Secure Client의 로밍 모듈을 시작하고 DNS 및/또는 웹 보호를 사용하려는 경우 Secure Client User Interface에서 오류 상태가 표시될 수 있습니다.

웹 보호 상태에 대해 클라우드 서비스 사용 불가



DNS 보호 상태에 대해 보호되지 않음



이러한 오류의 원인은 로밍 모듈이 네트워크 연결 문제로 인해 클라우드 서비스에 연결할 수 없기 때문입니다.

과거에 영향을 받는 클라이언트 PC에서 이 문제가 나타나지 않았다면 PC가 연결된 네트워크가 대부분 제한되어 있고 SSE 문서에 설명된 요구 사항을 충족하지 못했을 것입니다

## DNS 보호 상태가 보호되지 않음

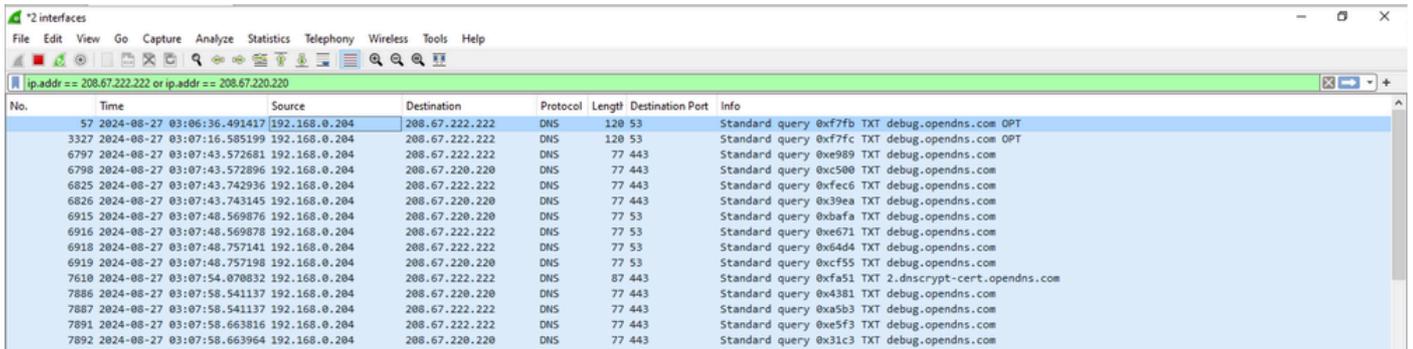
보호되지 않은 DNS 상태가 표시되면 대부분의 로밍 모듈은 OpenDNS 서버에 대한 업스트림 연결이 없을 것입니다(208.67.222.222 및 208.67.220.220).

DART 번들의 일부인 cscumbrellaplugin.txt 파일에 로그가 표시됩니다.

```
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
```

연결 문제를 다시 확인하고 확인하기 위해 PC(WiFi 또는 이더넷)의 이그레스 물리적 인터페이스에서 wireshark 캡처를 수집하고, 디스플레이 필터를 사용하여 OpenDNS 리졸버로 향하는 트래픽만 확인할 수 있습니다.

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



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 0xc555 TXT debug.opendns.com
7610	2024-08-27 03:07:54.070832	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 0x4381 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

Wireshark의 스니펫에서 볼 수 있듯이, 클라이언트가 UDP 포트 443 및 53에서 208.67.222.222 및 208.67.220.220으로 향하는 DNS TXT 쿼리를 계속 재전송하지만 응답을 받지 못한다는 것은 분명합니다.

이러한 행동에는 여러 가지 이유가 있을 수 있습니다. 대부분의 경우 경계 방화벽 디바이스가 OpenDNS 서버에 대한 이그레스 DNS 트래픽을 차단하거나 특정 DNS 서버에 대한 트래픽만 허용합니다.

## 웹 보호 상태가 클라우드 서비스를 사용할 수 없음

Service Unavailable Web protection(서비스 사용 불가 웹 보호) 상태가 표시되면 대부분의 로밍 모듈은 Secure Web Gateway 서버에 대한 업스트림 연결이 없을 수 있습니다.

PC에 SWG 서버에 대한 IP 연결이 없는 경우 DART 번들의 일부인 Umbrella.txt 파일에 로그가 표

시됩니다.

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

더 자세히 조사하려면 패킷 캡처를 수집하여 PC가 SWG 서버와 연결되어 있지 않음을 증명합니다.  
터미널에서 명령을 실행하여 SWG IP 주소를 가져옵니다.

<#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

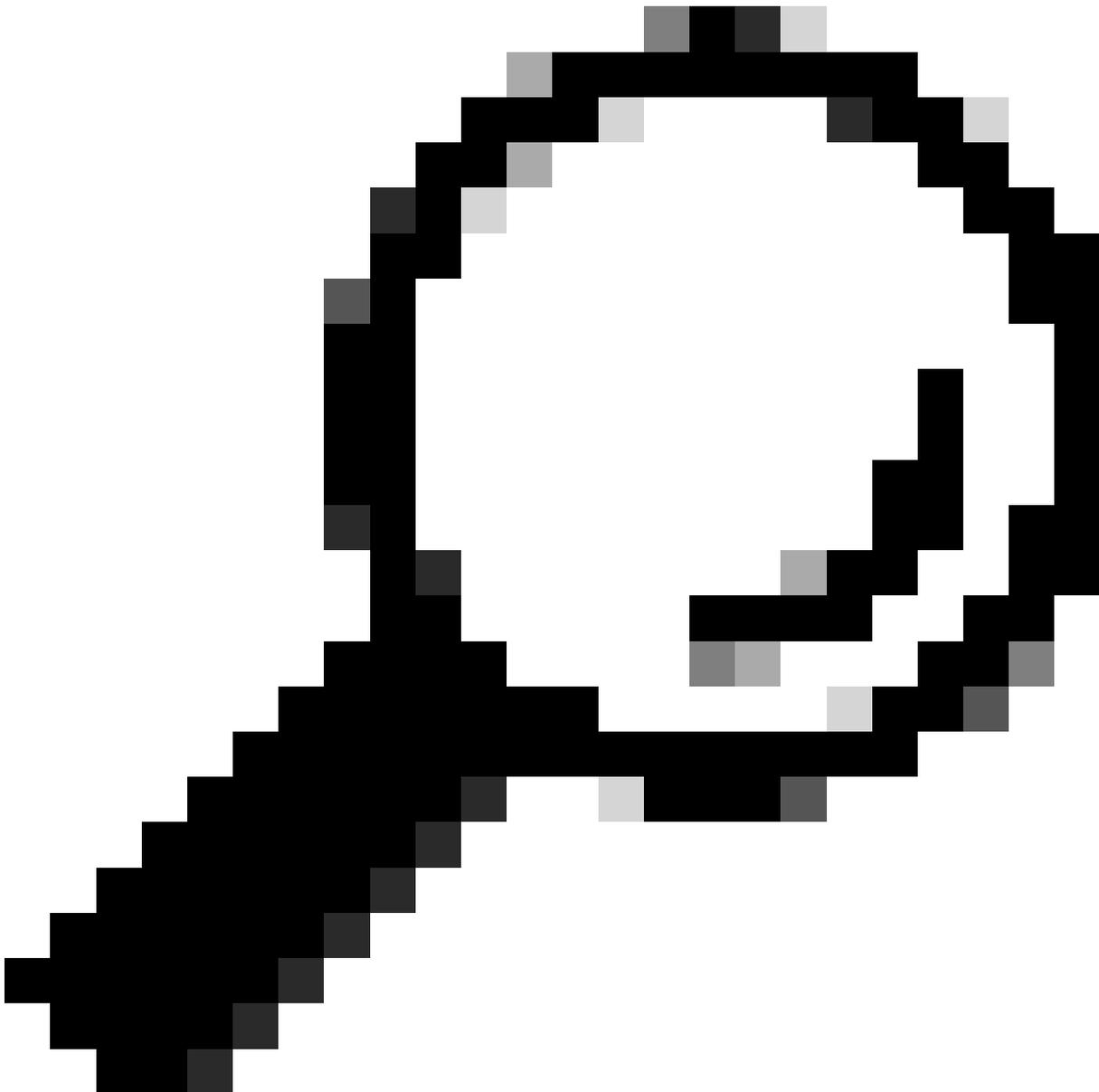
연결 문제를 다시 확인하고 확인하기 위해 PC의 이그레스 물리적 인터페이스(WiFi 또는 이더넷)에  
서 wireshark 캡처를 수집하고, 디스플레이 필터를 사용하여 SWG 서버로 향하는 트래픽만 살펴볼  
수 있습니다(이전 단계에서 얻은 IP 주소 사용)

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

Wireshark의 스니펫에서 볼 수 있듯이, 클라이언트가 18.135.112.200으로 향하는 TCP SYN 패킷을 계속 재전송하지만, 응답으로 TCP RST를 수신한다는 것은 분명합니다.

이 특정 실습 시나리오에서는 경계 방화벽이 SWG IP 주소에 대한 트래픽을 차단하고 있었습니다. 실제 시나리오에서는 TCP RST가 아니라 TCP SYN 재전송만 볼 수 있습니다.



---

팁: 클라이언트가 SWG 서버에 연결할 수 없는 경우, 기본적으로 웹 트래픽이 WiFi 또는 이더넷(Direct Internet Access)을 통해 나가는 fail open 상태를 입력합니다. 웹 보호는 실패 열기 모드에서 적용되지 않습니다.

---

## 솔루션

사용자는 기본 네트워크에서 문제가 발생하고 있음을 신속하게 파악하기 위해 경계 방화벽이 없는 다른 개방형 네트워크(핫스팟, 홈 WiFi)에 연결할 수 있습니다.

설명된 연결 오류를 수정하려면 SSE 설명서에 설명된 대로 PC에 제한 없는 업스트림 연결이 [있는지 확인하십시오](#).

DNS 보호 상태 문제:

- 208.67.222.222 TCP/UDP 포트 53
- 208.67.220.220 TCP/UDP 포트 53

웹 보호 상태 문제의 경우 인그레스 IP 주소에 대한 트래픽이 경계 방화벽에서 허용되는지 확인하십시오. - [SSE 문서](#)

특정 인그레스 IP 주소 범위는 위치에 따라 다릅니다.

## 관련 정보

- [Secure Access 사용 설명서](#)
- [Cisco Secure Client에서 DART 번들을 수집하는 방법](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.