

# Fehlerbehebung bei Secure Access-Roaming-Modul "Cloud-Service nicht verfügbar" oder "ungeschützt" Status

## Inhalt

---

[Einleitung](#)

[Problem](#)

[DNS-Schutzstatus ist ungeschützt](#)

[Status des Webschutzes ist Cloud-Dienst nicht verfügbar](#)

[Lösung](#)

[Zugehörige Informationen](#)

---

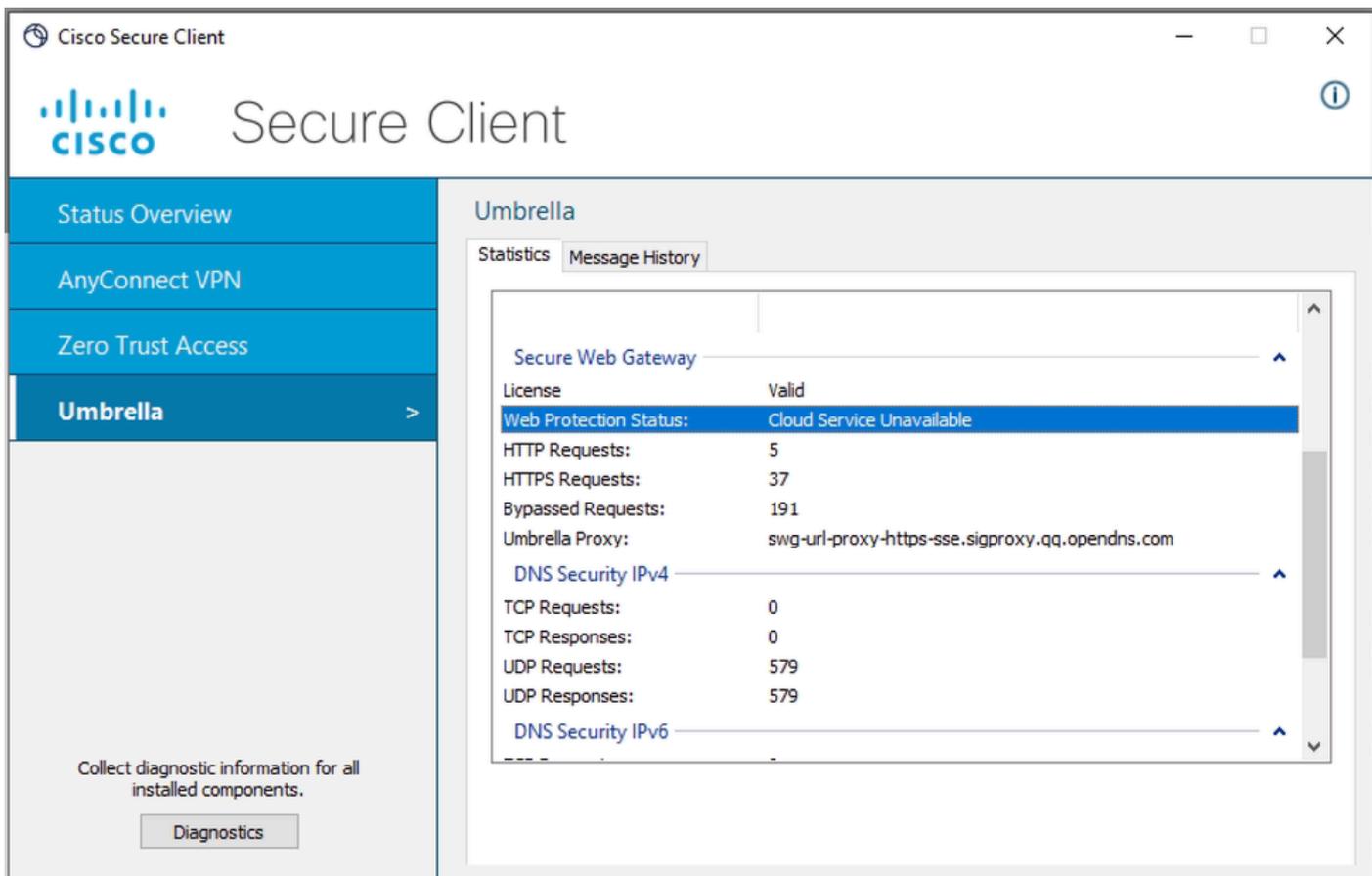
## Einleitung

Dieses Dokument beschreibt eine Möglichkeit, die Ursache des Status "Cloud-Service nicht verfügbar" oder "Nicht geschützt" im Roaming-Modul des sicheren Clients zu untersuchen.

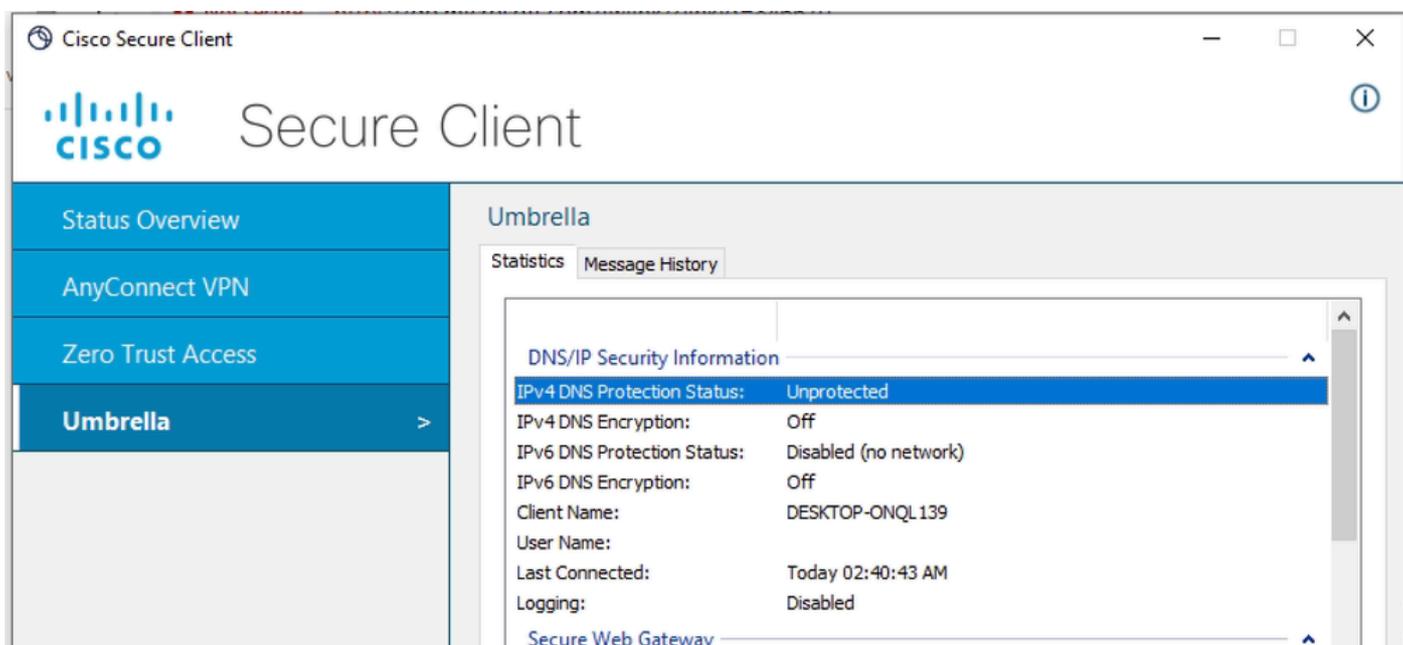
## Problem

Wenn ein Benutzer das Roaming-Modul des sicheren Clients startet und erwartet, DNS- und/oder Webschutz zu verwenden, können in der sicheren Client-Benutzeroberfläche fehlerhafte Zustände angezeigt werden:

Cloud-Service für Webschutzstatus nicht verfügbar



Unprotected for DNS Protection Status



Der Grund für diese Fehler ist, dass das Roaming-Modul aufgrund von Netzwerkverbindungsproblemen keine Verbindung zu seinen Cloud-Services herstellen kann.

Wenn dieses Problem auf dem betroffenen Client-PC in der Vergangenheit nicht aufgetreten ist, bedeutet dies, dass höchstwahrscheinlich das Netzwerk, mit dem der PC verbunden ist, eingeschränkt ist und die Anforderungen der [SSE-Dokumentation](#) nicht erfüllt.

## DNS-Schutzstatus ist ungeschützt

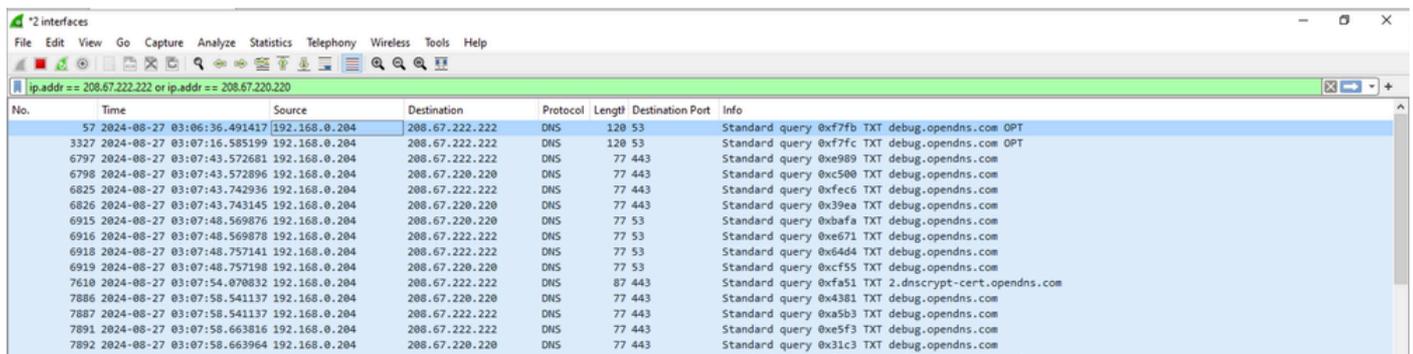
Wenn Sie Unprotected DNS state (Ungeschützter DNS-Status) sehen, hat das Roaming-Modul höchstwahrscheinlich keine Upstream-Verbindung zu OpenDNS-Servern (208.67.222.222 und 208.67.220.220).

Sie sehen die Datei cscumbrellaplugin.txt, die Teil des DART-Pakets ist.

```
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
```

Um Verbindungsprobleme zu überprüfen und zu bestätigen, können Sie die Erfassung von Wireshark an der physischen Ausgangsschnittstelle des PCs (WiFi oder Ethernet) erfassen und den Anzeigefilter verwenden, um nur nach Datenverkehr zu suchen, der an OpenDNS-Resolver gerichtet ist:

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



The screenshot shows a Wireshark capture window with the filter 'ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220'. The packet list pane displays a series of DNS standard queries (TXT) to debug.opendns.com. The source IP is consistently 192.168.0.204, and the destination IP is either 208.67.222.222 or 208.67.220.220. The queries are for various TXT records, including '0xf7fb', '0xf7fc', '0xe989', '0xc500', '0xfec6', '0x39ea', '0xbafa', '0xe671', '0x64d4', '0xcf55', '0xfa51', '0x43b1', '0xa5b3', and '0xe5f3'. The length of the queries varies between 53 and 128 bytes.

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	128	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	128	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 03:07:54.070832	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 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

Wie Sie im Ausschnitt von Wireshark sehen können, ist es klar, dass der Client auf UDP-Port 443 und 53 DNS-TXT-Abfragen, die an 208.67.222.222 und 208.67.220.220 gerichtet sind, immer wieder sendet, jedoch keine Antwort erhält.

Für ein solches Verhalten kann es mehrere Gründe geben: Wahrscheinlich blockiert das Perimeter-Firewall-Gerät den ausgehenden DNS-Datenverkehr zu OpenDNS-Servern oder lässt nur Datenverkehr zu bestimmten DNS-Servern zu.

## Status des Webschutzes ist Cloud-Dienst nicht verfügbar

Wenn der Status "Service Unavailable Web Protection" (Dienst nicht verfügbar) angezeigt wird, verfügt das Roaming-Modul höchstwahrscheinlich nicht über Upstream-Verbindungen zu Secure

Web Gateway-Servern.

Wenn der PC keine IP-Verbindung zu den SWG-Servern hat, wird die Datei Umbrella.txt angezeigt, die Teil des DART-Pakets ist.

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

Sammeln Sie zur weiteren Untersuchung die Paketerfassung, um zu beweisen, dass der PC keine Verbindung zum SWG-Server hat.

Geben Sie den Befehl im Terminal ein, um die SWG-IP-Adresse zu erhalten:

<#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

Um Verbindungsprobleme doppelt zu überprüfen und zu bestätigen, können Sie die Erfassung von Wireshark an der physischen Ausgangsstelle des PCs (WiFi oder Ethernet) erfassen und mithilfe des Anzeigefilters nur nach Datenverkehr suchen, der an den SWG-Server gerichtet ist (verwenden Sie die im vorherigen Schritt erhaltene IP-Adresse).

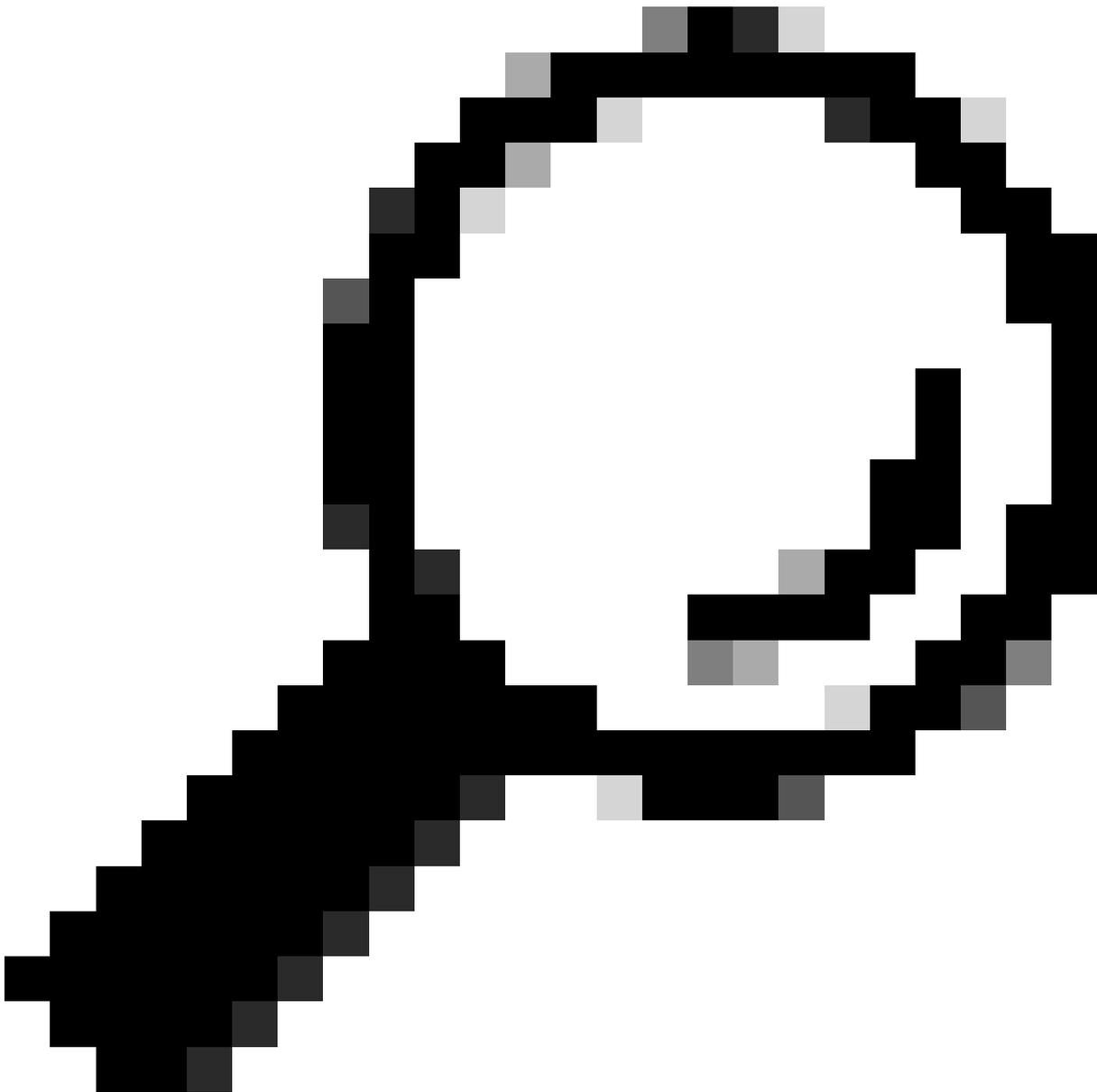
ip.addr == 18.135.112.200

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

Wie Sie im Ausschnitt von Wireshark sehen können, ist klar, dass der Client TCP-SYN-Pakete, die an 18.135.112.200 gerichtet sind, immer wieder sendet, aber als Antwort TCP-RST empfängt.

In diesem speziellen Lab-Szenario blockierte die Perimeter-Firewall den Datenverkehr zur SWG-IP-Adresse.

In der Praxis können Sie nur TCP SYN-Neuübertragungen sehen, nicht TCP RST.



Tipp: Wenn der Client die SWG-Server nicht erreichen kann, wechselt er standardmäßig in den Fail-Open-Status, in dem der Web-Datenverkehr über den direkten Internetzugang (Wi-Fi oder Ethernet) abfließt. Der Webschutz wird im Fail-Open-Modus nicht angewendet.

---

## Lösung

Um schnell zu erkennen, dass das zugrunde liegende Netzwerk Probleme verursacht, kann der Benutzer eine Verbindung zu jedem anderen offenen Netzwerk (Hotspot, privates WiFi) herstellen, das keine Perimeter-Firewall hat.

Um den beschriebenen Verbindungsfehler zu beheben, stellen Sie sicher, dass der PC über eine uneingeschränkte Upstream-Konnektivität verfügt, wie in der [SSE-Dokumentation](#) beschrieben.

Probleme mit dem DNS-Schutzstatus:

- 208.67.222.222 TCP/UDP-Port 53
- 208.67.220.220 TCP/UDP-Port 53

Stellen Sie bei Problemen mit dem Web-Schutzstatus sicher, dass der Datenverkehr zu den Eingangs-IP-Adressen auf der Perimeter-Firewall zulässig ist - [SSE-Dokumentation](#)

Der spezifische Bereich der Eingangs-IP-Adressen hängt von Ihrem Standort ab.

## Zugehörige Informationen

- [Benutzerhandbuch zu Secure Access](#)
- [Sammeln Sie das DART-Paket vom Cisco Secure Client.](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.