

# Probleemoplossing voor Secure Access Roaming Module "a;cloudservice niet beschikbaar&vragen; of "a;onbeveiligd&vragen; status

## Inhoud

---

[Inleiding](#)

[Probleem](#)

[DNS-beschermingsstatus is onbeveiligd](#)

[Web Protection Status is niet beschikbaar voor cloudservice](#)

[Oplossing](#)

[Gerelateerde informatie](#)

---

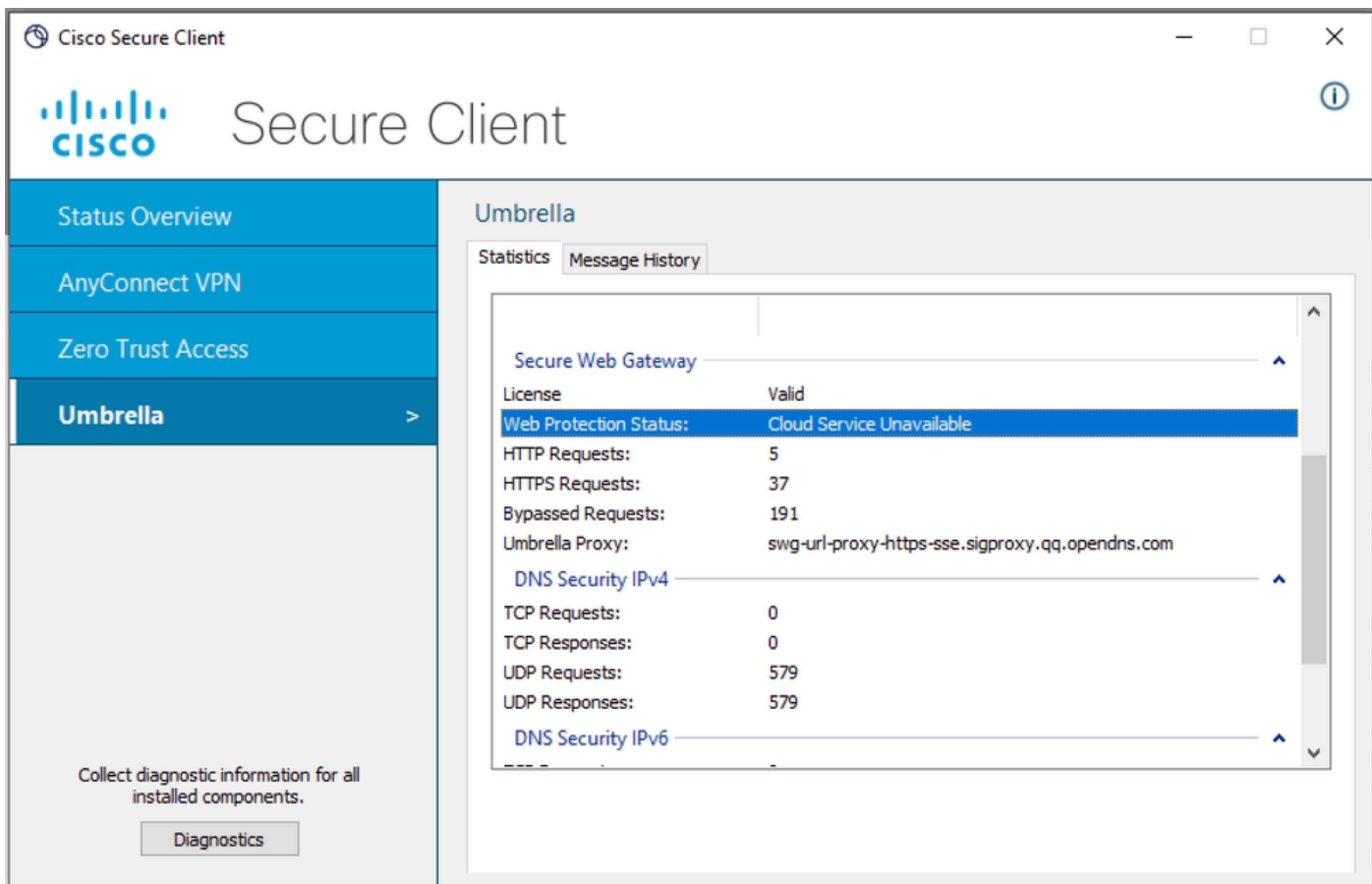
## Inleiding

Dit document beschrijft een manier om de grondoorzaak van de status "Cloud Service niet beschikbaar" of "onbeschermd" in Roaming Module van Secure Client te onderzoeken.

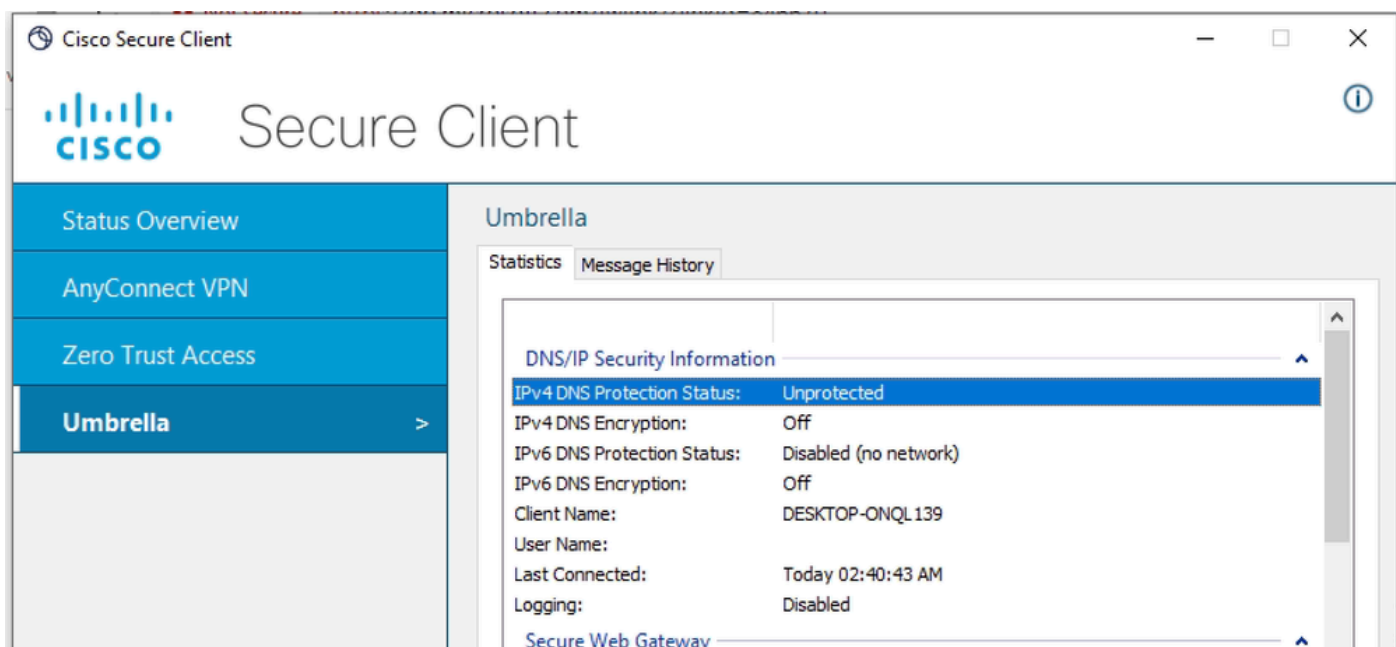
## Probleem

Wanneer een gebruiker roamingmodule van Secure Client start en verwacht DNS en/of webbeveiliging te gebruiken, kunnen in Secure Client User Interface foutieve toestanden worden waargenomen:

Cloud-service niet beschikbaar voor webbeschermingsstatus



Onbeschermd voor DNS-beschermingsstatus



De reden voor deze fouten is dat Roaming Module geen contact kan opnemen met zijn clouddiensten vanwege problemen met netwerkconnectiviteit.

Als dit probleem zich in het verleden niet op de betreffende client-pc heeft voorgedaan, betekent dit dat het netwerk waarmee de pc is verbonden, hoogstwaarschijnlijk beperkt is en niet voldoet aan de vereisten die in [SSE-documentatie](#) worden beschreven

## DNS-beschermingsstatus is onbeveiligd

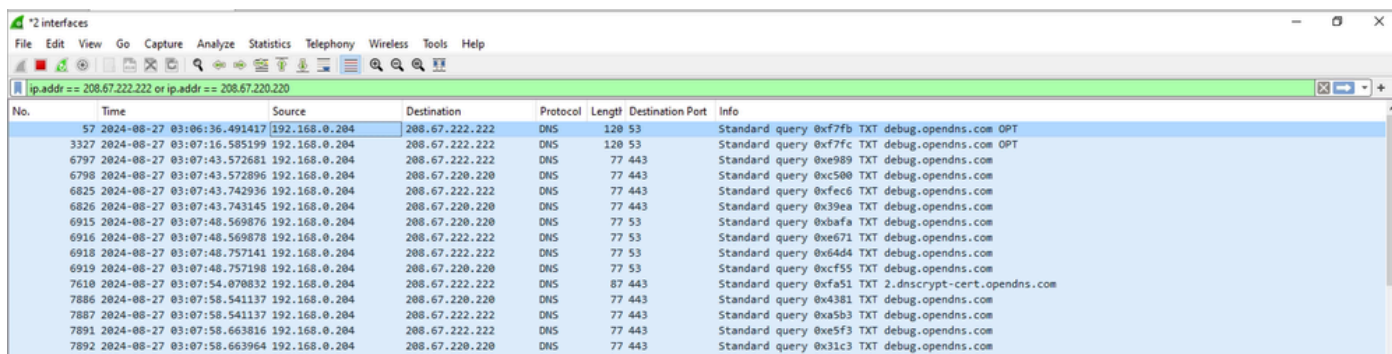
Wanneer u onbeschermd DNS staat ziet, dan heeft de het meest waarschijnlijke het Zwerven Module geen stroomopwaartse connectiviteit aan servers OpenDNS (208.67.222.222 en 208.67.220.220).

Je zou het inloggen cscumbrellaplugin.txt bestand zien, dat deel uitmaakt van DART bundel.

```
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
```

Om connectiviteitsproblemen te controleren en te bevestigen kunt u wireshark-opname verzamelen op de uitgaande fysieke interface van de PC (WiFi of Ethernet) en het weergavefilter gebruiken om alleen te zoeken naar verkeer dat bestemd is voor OpenDNS-oplossers:

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



The image shows a Wireshark capture window with a filter applied: 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 destination port is 53 for all queries.

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 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

Zoals u ziet in het fragment van Wireshark, is het duidelijk dat client blijft herverzenden DNS TXT-vragen die zijn bestemd voor 208.67.222.222 en 208.67.220.220 op UDP-poort 443 en 53, maar geen antwoord ontvangt.

Er kunnen meerdere redenen achter dergelijk gedrag zijn, de perimeter firewall-apparaat blokkeert hoogstwaarschijnlijk het uitgaande DNS-verkeer naar OpenDNS-servers, of laat alleen verkeer toe naar een specifieke DNS-servers.

## Web Protection Status is niet beschikbaar voor cloudservice

Als u ziet dat er geen service beschikbaar is voor de status van de webbeveiliging, dan is er waarschijnlijk geen upstream-verbinding met Secure Web Gateway-servers.

Als PC geen IP-verbinding met SWG-servers heeft, ziet u het inlogbestand Umbrella.txt, dat deel uitmaakt van DART-bundel.

```
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
```

Om verder te onderzoeken, verzamel pakketopname om te bewijzen dat PC geen connectiviteit met de server van SWG heeft.

Geef het bevel in terminal uit om SWG IP adres te krijgen:

```
<#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
```

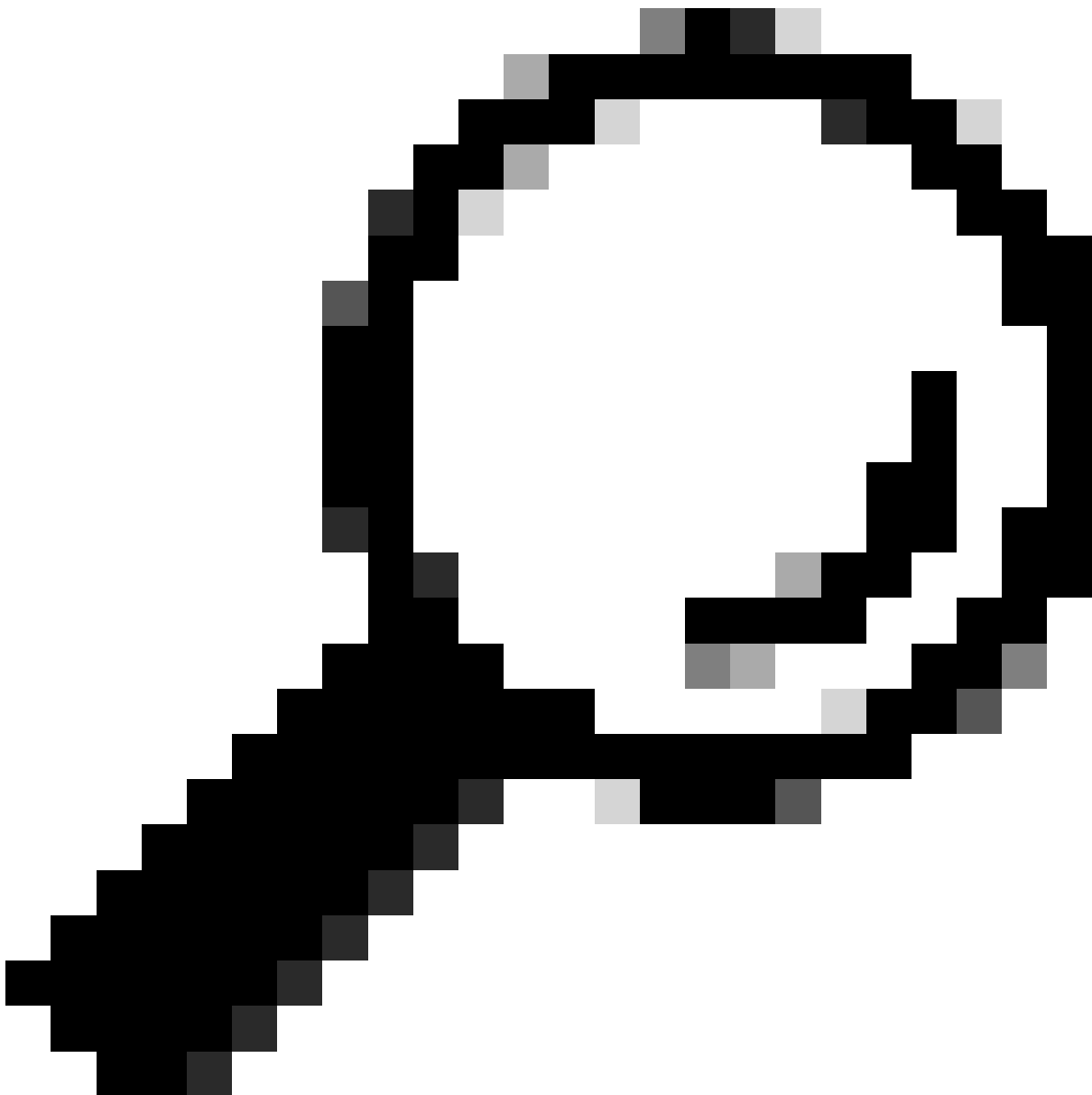
Om connectiviteitsproblemen te controleren en te bevestigen, kunt u Wireshark Capture verzamelen op de uitgaande fysieke interface van de PC (WiFi of Ethernet) en weergavefilter gebruiken om alleen te zoeken naar verkeer dat is bestemd voor SWG-server (gebruik IP-adres dat in de vorige stap is verkregen)

```
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 06:41:20.603745	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

Zoals u in het fragment van Wireshark ziet, is het duidelijk dat de client TCP SYN-pakketten die zijn bestemd voor 18.135.112.200 opnieuw doorsturen, maar als reactie TCP RST ontvangt.

In dit specifieke labscenario blokkeerde de perimeterfirewall het verkeer naar SWG IP-adres. In real-life scenario, kunt u slechts TCP SYN heruitzendingen zien, niet TCP RST.



---

Tip: Als client geen SWG-servers kan bereiken, wordt standaard de failliete open status ingevoerd waar webverkeer via Direct Internet Access (WiFi of Ethernet) vertrekt. Web bescherming wordt niet toegepast in de failliete open modus.

---

## Oplossing

Om snel te kunnen vaststellen dat het onderliggende netwerk problemen veroorzaakt, kan de gebruiker verbinding maken met een ander open netwerk (hotstop, home WiFi) dat geen perimeterfirewall heeft.

Om de beschreven verbindingfout op te lossen, dient u ervoor te zorgen dat de PC beschikt over onbeperkte upstream connectiviteit zoals beschreven in [SSE Documentatie](#).

Problemen met DNS-beschermingsstatus:

- 208.67.22.22 TCP/UDP-poort 53
- 208.67.220.220 TCP/UDP-poort 53

Zorg er bij problemen met de webbeschermingsstatus voor dat verkeer naar Ingress IP-adressen is toegestaan in een firewall op het perimeter - [SSE Documentatie](#)

Specifieke bereik van Ingress IP-adressen is afhankelijk van uw locatie.

## Gerelateerde informatie

- [Gebruikershandleiding voor Secure Access](#)
- [Hoe u een DART-bundel kunt verzamelen bij Cisco Secure-client](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.