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

Inhoud

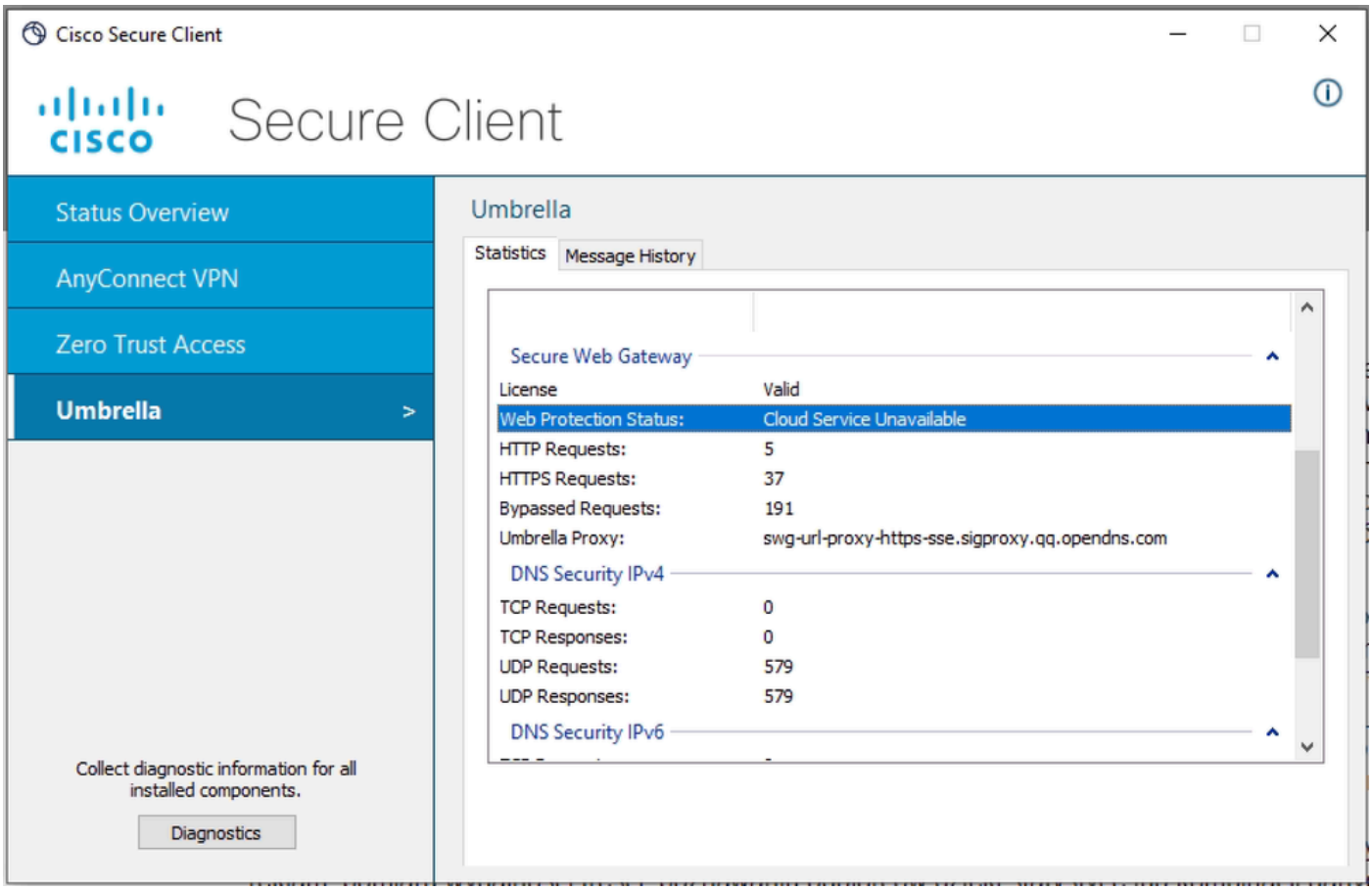
Inleiding

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.

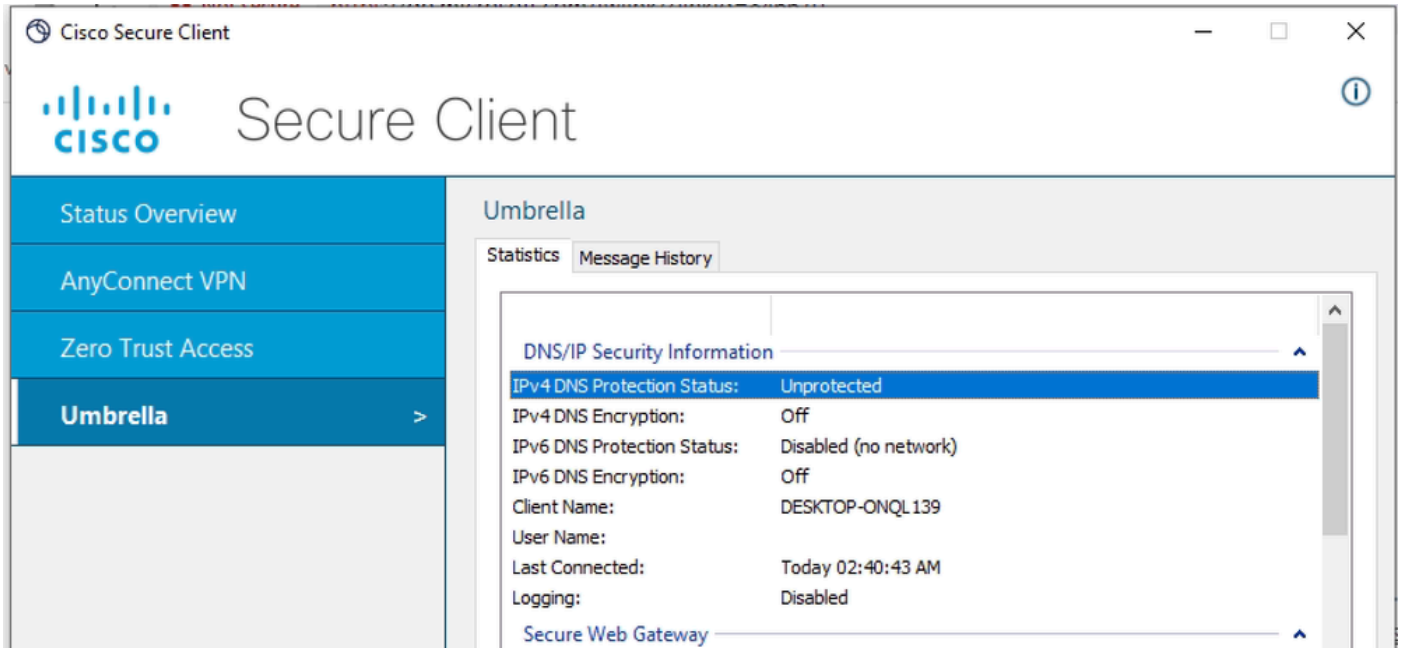
Probleem

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

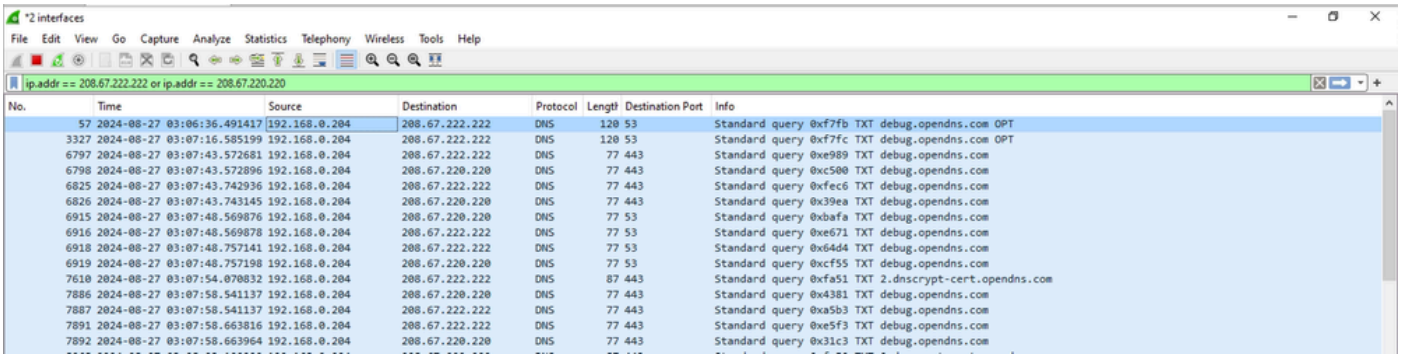
DNS-beschermingsstatus is onbeveiligd

Wanneer u onbeschermde 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
```



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.

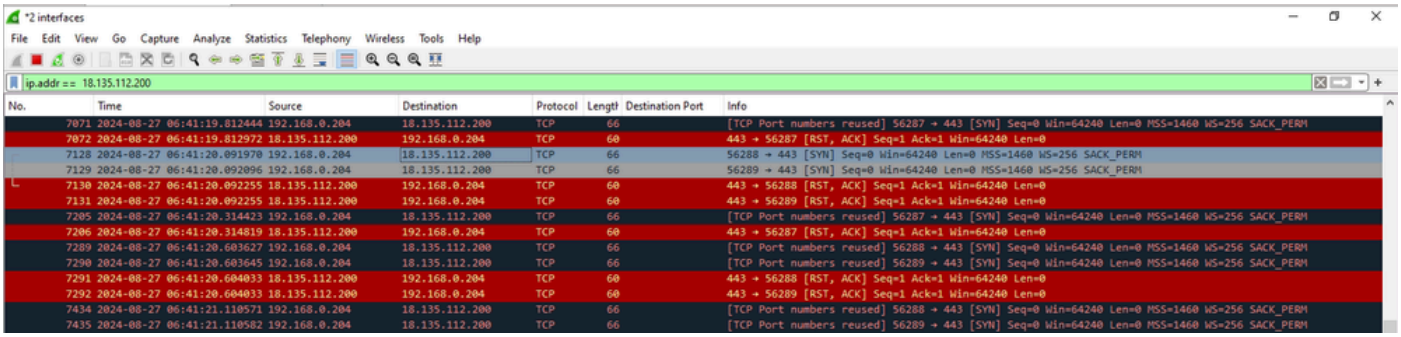
```
Date : 08/27/2024
Time : 06:41:22
Type : Warning
Source : csc_swgagent

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
```

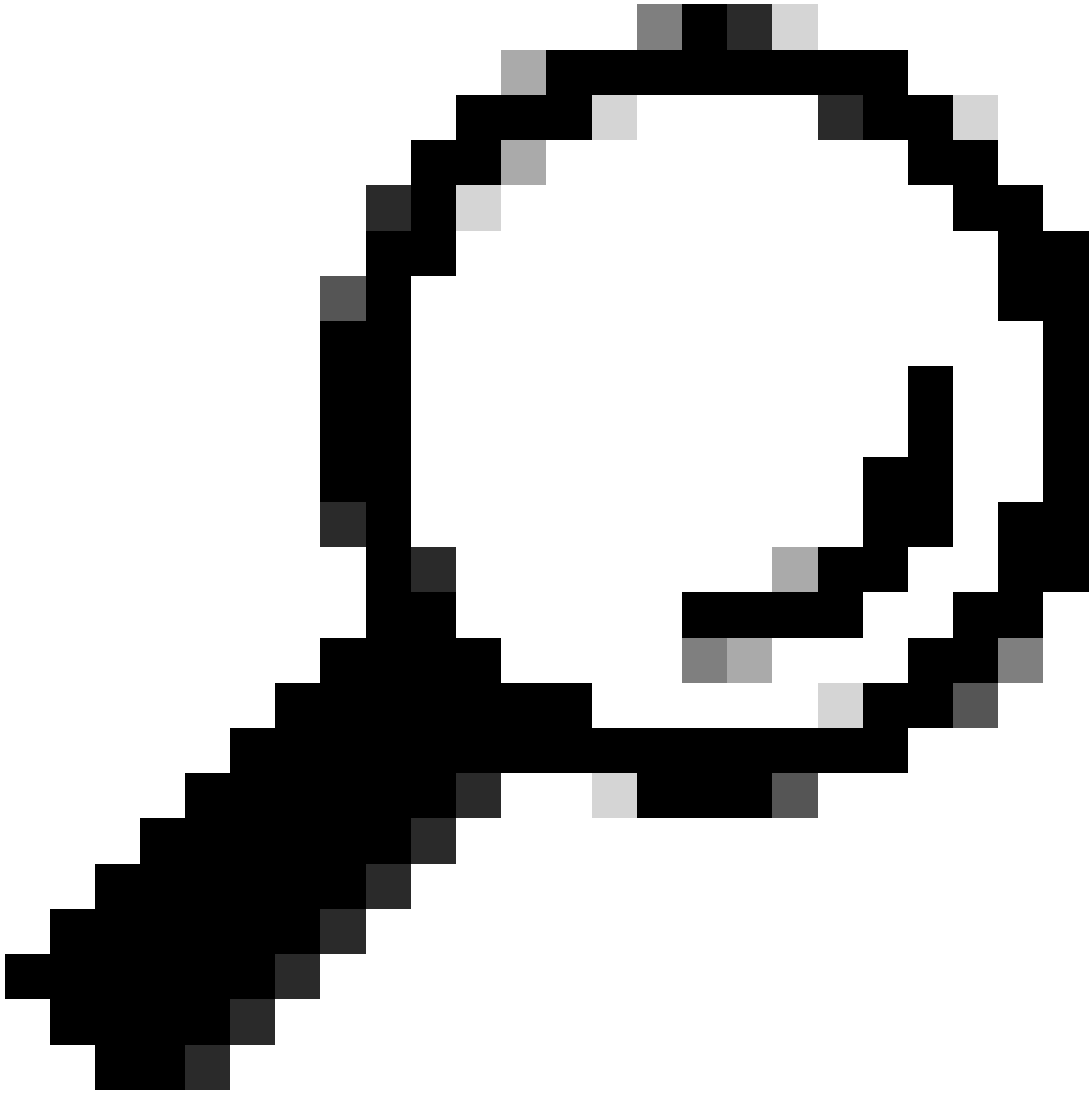
Om connectiviteitsproblemen te controleren en te bevestigen, kunt u wireshark Capture verzamelen op de uitgaande fysieke interface van de PC (WiFi of Ethernet) en weergavefilter gebruiken om alleen te zoeken naar verkeer dat is bestemd voor SWG-server (gebruik IP-adres dat in de vorige stap is verkregen)

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



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 verbindingsfout 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.