Dépannage de l'état du module d'itinérance d'accès sécurisé " ; Service cloud indisponible " ; ou " ; Non protégé" ;

Table des matières

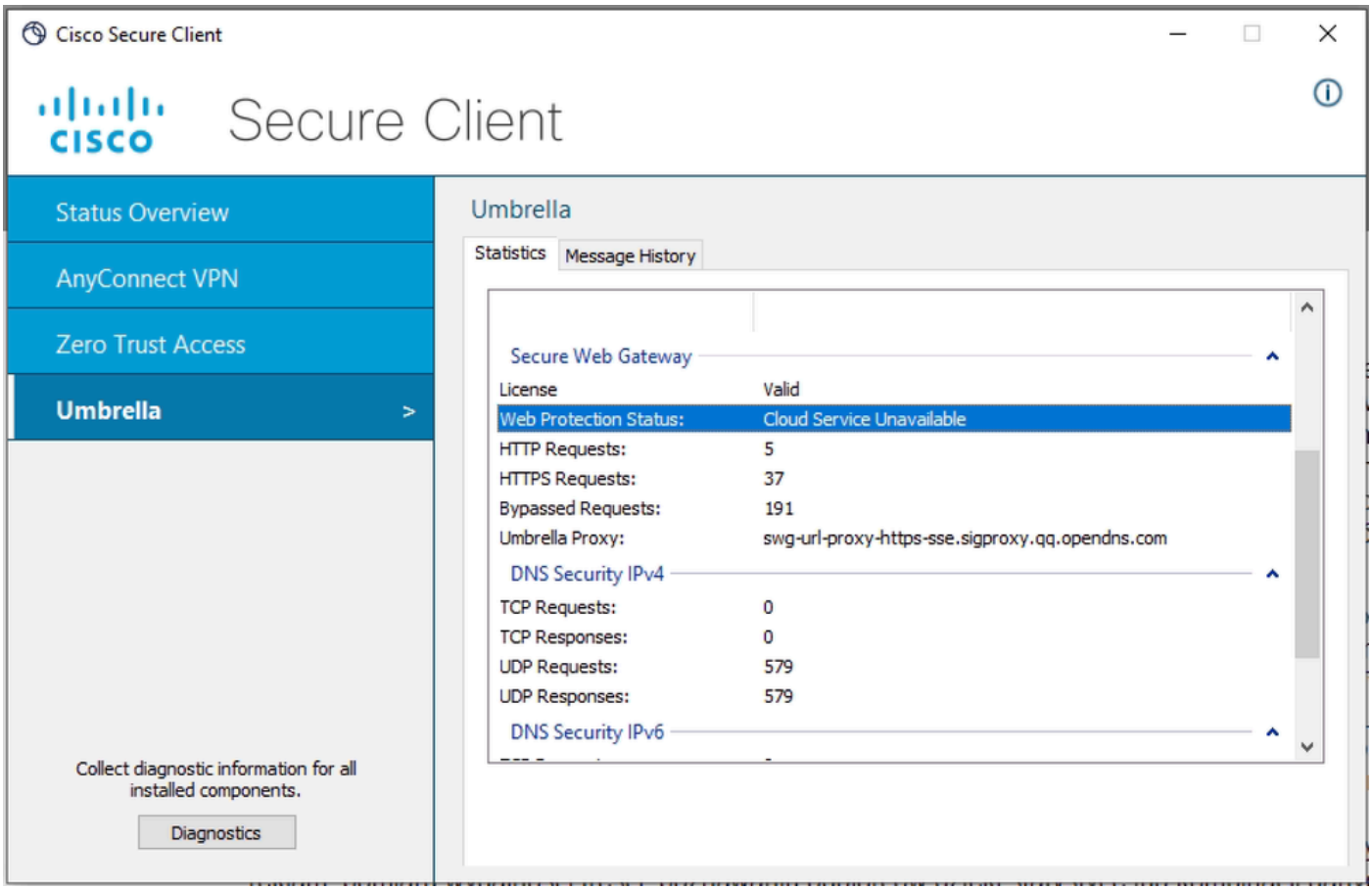
Introduction

Ce document décrit une façon d'enquêter sur la cause racine de l'état "Service cloud indisponible" ou "non protégé" dans le module d'itinérance du client sécurisé.

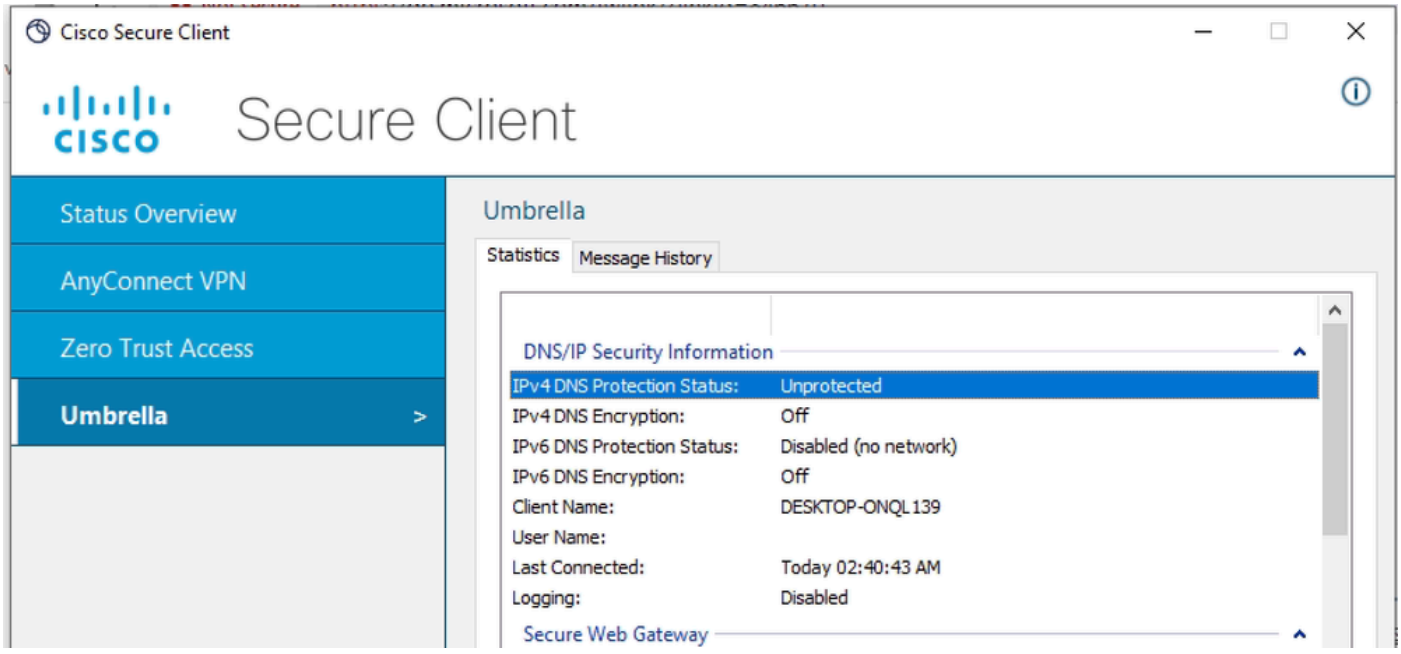
Problème

Lorsqu'un utilisateur lance le module d'itinérance du client sécurisé et s'attend à utiliser la protection DNS et/ou Web, des états erronés peuvent être observés dans l'interface utilisateur du client sécurisé :

Service cloud non disponible pour l'état de protection Web



Non protégé pour l'état de protection DNS



La raison de ces erreurs est que le module d'itinérance ne peut pas contacter ses services cloud en raison de problèmes de connectivité réseau.

Si ce problème n'a pas été détecté sur le PC client concerné par le passé, cela signifie très probablement que le réseau auquel le PC est connecté est restreint et ne répond pas aux exigences décrites dans la documentation SSE

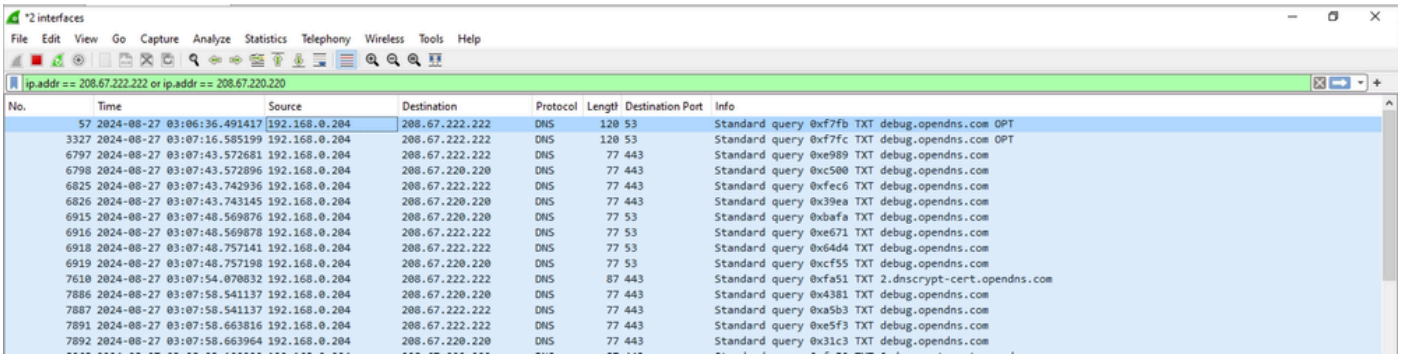
L'état de protection DNS est Non protégé

Lorsque vous voyez l'état DNS non protégé, alors très probablement le module d'itinérance n'a pas de connectivité en amont aux serveurs OpenDNS (208.67.222.222 et 208.67.220.220). Vous verriez le journal dans le fichier cscumbrellaplugin.txt, qui fait partie du bundle DART.

```
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
```

Afin de vérifier et de confirmer les problèmes de connectivité, vous pouvez collecter la capture Wireshark sur l'interface physique de sortie du PC (WiFi ou Ethernet), et utiliser le filtre d'affichage pour rechercher uniquement le trafic destiné aux résolveurs OpenDNS :

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



Comme vous le voyez dans l'extrait de Wireshark, il est clair que le client continue de retransmettre des requêtes DNS TXT destinées à 208.67.222.222 et 208.67.220.220 sur les ports UDP 43 et 53, mais ne reçoit aucune réponse.

Il peut y avoir plusieurs raisons derrière un tel comportement, le plus probablement périphérique pare-feu de périmètre bloque le trafic DNS de sortie vers les serveurs OpenDNS, ou autorise seulement le trafic vers un serveur DNS spécifique.

L'état de la protection Web est Service cloud indisponible

Lorsque l'état de protection Web Service non disponible s'affiche, il est très probable que le module d'itinérance ne dispose pas d'une connectivité en amont vers les serveurs de passerelle Web sécurisée.

Si l'ordinateur n'a pas de connectivité IP aux serveurs SWG, vous verriez le journal dans le fichier Umbrella.txt, qui fait partie de l'offre groupée DART.

```
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
```

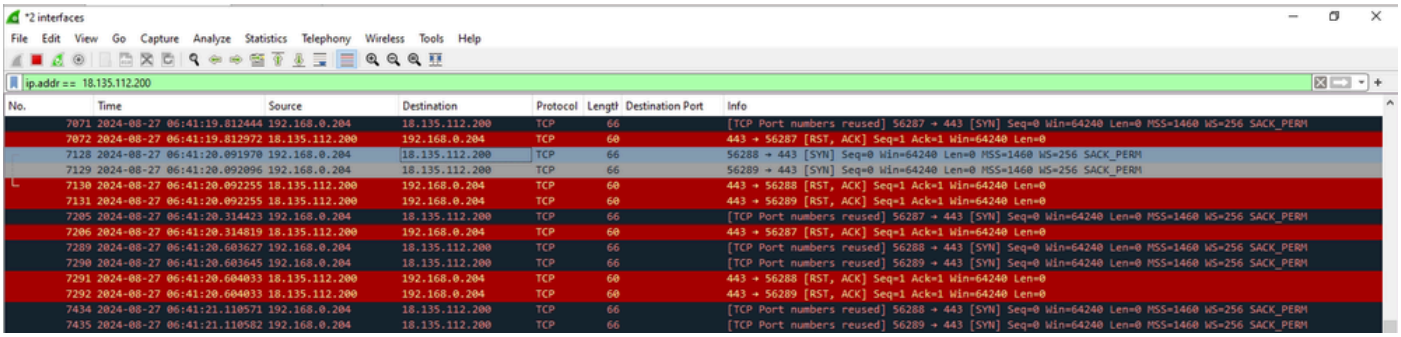
Afin d'étudier plus en détail, collectez la capture de paquets pour prouver que le PC n'a pas de connectivité avec le serveur SWG.
Exécutez la commande dans terminal pour obtenir l'adresse IP SWG :

<#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
```

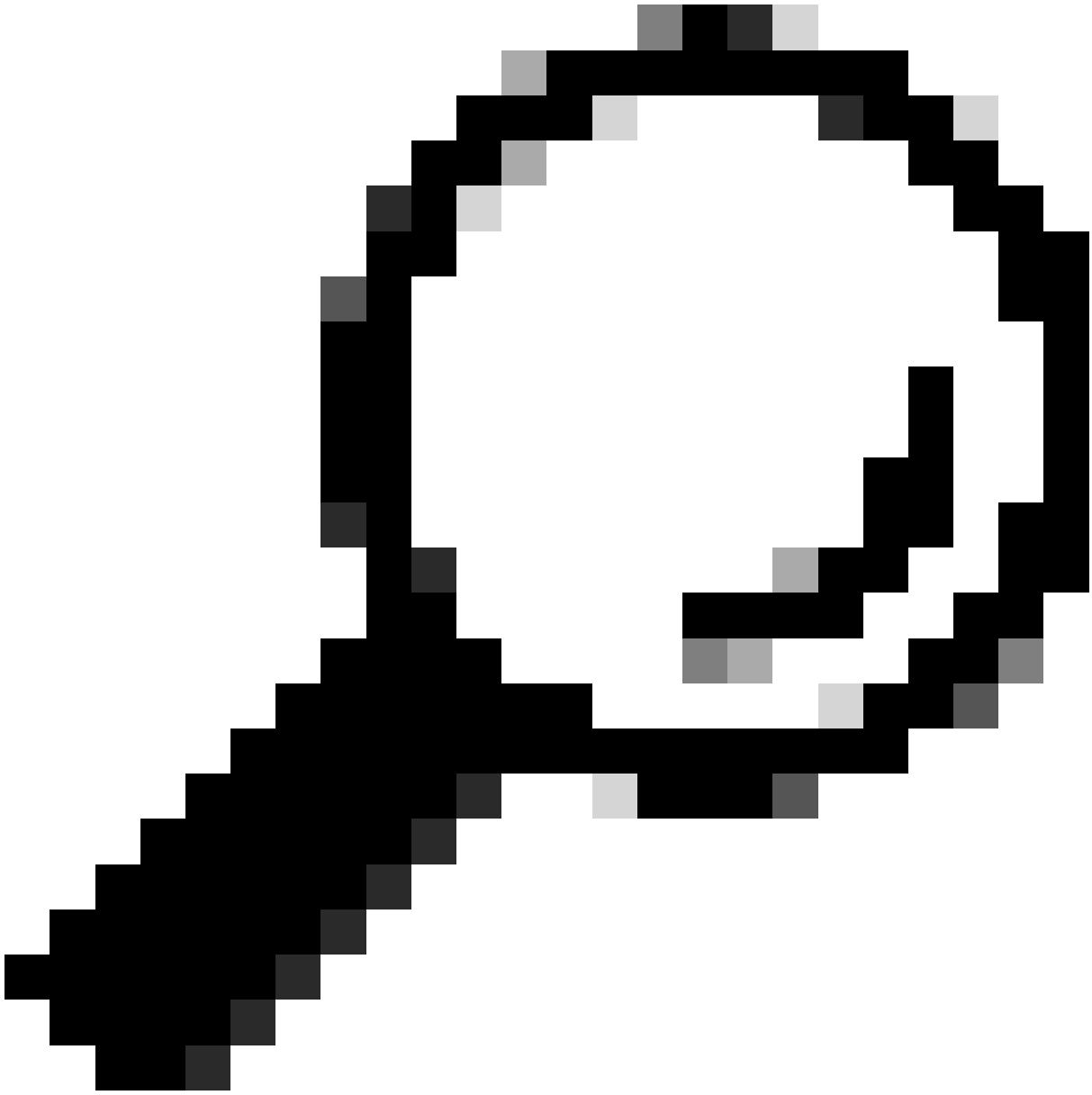
Afin de vérifier et de confirmer les problèmes de connectivité, vous pouvez collecter la capture Wireshark sur l'interface physique de sortie du PC (WiFi ou Ethernet), et utiliser le filtre d'affichage pour rechercher uniquement le trafic destiné au serveur SWG (utiliser l'adresse IP obtenue à l'étape précédente)

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



Comme vous le voyez dans l'extrait de Wireshark, il est clair que le client continue de retransmettre des paquets SYN TCP destinés à 18.135.112.200, mais reçoit TCP RST comme réponse.

Dans ce scénario de travaux pratiques spécifique, le pare-feu de périmètre bloquait le trafic vers l'adresse IP SWG.
Dans un scénario réel, vous ne pouvez voir que les retransmissions TCP SYN, pas TCP RST.



Conseil : si le client ne parvient pas à atteindre les serveurs SWG, il passe par défaut à l'état fail open où le trafic Web part via Direct Internet Access (WiFi ou Ethernet). La protection Web n'est pas appliquée en mode fail open.

Solution

Afin d'identifier rapidement que le réseau sous-jacent est à l'origine des problèmes, l'utilisateur peut se connecter à tout autre réseau ouvert (hotstop, WiFi domestique) qui n'a pas de pare-feu de périmètre.

Pour corriger l'erreur de connexion décrite, assurez-vous que le PC dispose d'une connectivité ascendante illimitée, comme indiqué dans la documentation SSE.

Problèmes d'état de protection DNS :

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

Pour les problèmes d'état de protection Web, assurez-vous que le trafic vers les adresses IP d'entrée est autorisé sur le pare-feu de périmètre - Documentation SSE

La plage spécifique d'adresses IP d'entrée dépend de votre emplacement.

Informations connexes

- Guide de l'utilisateur Secure Access
- Comment collecter le bundle DART auprès de Cisco Secure Client
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.