

Fehlerbehebung bei Verbindungen mit Hotspots über Captive Portal mit aktiviertem AnyConnect SWG-Modul

Inhalt

[Einleitung](#)

[Problem](#)

[Korrekturen und Empfehlungen für weitere Fehlerbehebung](#)

[Konfigurieren von Antivirus-Anwendungen für AnyConnect](#)

[Details](#)

[Versionen vor 4.10.05095](#)

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei Verbindungen zu Hotspots über Captive Portal mit aktiviertem AnyConnect SWG-Modul.

Problem

Benutzer mit dem AnyConnect Secure Web Gateway (SWG)-Modul können sich möglicherweise nicht an einigen öffentlichen Hotspots anmelden.

Korrekturen und Empfehlungen für weitere Fehlerbehebung

Stellen Sie sicher, dass Sie AnyConnect Version 4.10.05095 (4.10MR5) verwenden. In dieser Version werden Probleme im Zusammenhang mit dem Captive Portal behandelt.

Sollte das Problem jedoch auch nach dem Upgrade auf 4.10.05095 weiterhin bestehen, wenden Sie sich bitte an den Umbrella Support.

Um den Support-Prozess zu beschleunigen, bitten wir die Kunden, diese Schritte durchzugehen und die angeforderten Protokolle zu sammeln, bevor sie sich an den Umbrella Support wenden.

1. Wir fordern Kunden auf, alle auf ihren Endgeräten installierten Sicherheitsagenten so zu konfigurieren, dass sie AnyConnect-Binärdateien und -Verbindungen ausschließen, um Richtlinienkonflikte zu vermeiden. Daher müssen TrendMicro und/oder andere Sicherheitsagenten entsprechend konfiguriert werden.
Lesen Sie den entsprechenden Ausschnitt aus den AnyConnect-[Versionshinweisen](#), und stellen Sie sicher, dass die Ausnahmen für AnyConnect entsprechend gemacht werden.
2. Rufen Sie HTTP-URLs (z. B. <http://www.portquiz.net>) und HTTPS-URLs (<https://www.google.com>) im Browser auf, und prüfen Sie, ob die Umleitung zum Captive

Portal erfolgt.

3. Wenn das Problem weiterhin besteht, sammeln Sie ein DART-Paket (maximal Debug aktiviert), eine PCAP-Datei (einschließlich Loopback) und eine Bildschirmaufzeichnung (optional), um das Problem weiter zu untersuchen.

Konfigurieren von Antivirus-Anwendungen für AnyConnect

Anwendungen wie Antivirus, Anti-Malware und Intrusion Prevention System (IPS) können das Verhalten von AnyConnect Secure Mobility Client-Anwendungen als schädlich interpretieren. Sie können Ausnahmen konfigurieren, um solche Fehlinterpretationen zu vermeiden. Konfigurieren Sie nach der Installation der AnyConnect-Module oder -Pakete Ihre Antivirus-Software so, dass der AnyConnect-Installationsordner zugelassen wird, oder stellen Sie Sicherheitsausnahmen für die AnyConnect-Anwendungen her. Die allgemeinen Verzeichnisse, die ausgeschlossen werden sollen, sind aufgeführt, obwohl die Liste möglicherweise nicht vollständig ist:

- C:\Users<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Dateien (x86)\Cisco

Details

Captive Portal-Probleme können durch [CSCwb39828](#) verursacht werden. "Captive Portal-Seite wurde nicht geöffnet, wenn SWG für Fail Open/Fail Close aktiviert ist". Nach dem Upgrade auf AnyConnect 4.10.05095 ist keine weitere Konfiguration oder Benutzerinteraktion erforderlich.

Einige Wireless-Hotspots und andere Gastnetzwerke unterbrechen den Internetzugriff und leiten den Internetverkehr an ein Captive Portal (manchmal auch als Walled Garden bezeichnet) weiter. AnyConnect SWG-Versionen vor 4.10.05095 könnten versuchen, diesen Web-Datenverkehr an die Umbrella Cloud zu senden, auch wenn kein Internetzugang verfügbar ist, was das System daran hindert, lokal mit dem Captive Portal zu interagieren. Diese lokale Interaktion kann erforderlich sein, um den Zugriff durch Authentifizierung, Zahlung oder eine Click-through-Vereinbarungsseite zu gewähren.

Versionen vor 4.10.05095

Die Unterstützung für Captive Portals mit früheren Versionen von AnyConnect ist bei Verwendung von SWG beschränkt. Diese Aktionen eines Captive Portals machen es für einen SWG-Client wahrscheinlich unerreichbar:

- Umleitung zu oder Laden von Ressourcen von einem Ziel außerhalb des privaten IP-Adressbereichs von RFC-1918.
- Akzeptieren eines TCP-Handshakes für Umbrella-Proxys auf Port 80 oder 443 und dann Schließen der Verbindung oder Bereitstellen einer unerwarteten Antwort.

Fügen Sie zur Problemumgehung im Abschnitt Deployments → Domain Management → External Domains & IPs (Bereitstellungen → Domänenmanagement → Externe Domänen und

IPs) des Umbrella Dashboards für jedes Ziel, das nicht geladen werden kann, Ausnahmen hinzu. Das Verhalten des Captive Portals ist implementierungsspezifisch, daher variieren die erforderlichen Umleitungsdomänen oder IP-Adressen je nach Hotspot.

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.