Der VPN-Client konnte den Fehler bei der Änderung der IP-Weiterleitungstabelle auf nicht erfolgreich überprüfen Secure Client RAVPN Split-Tunnel/Standard-DNS

Inhalt

Problem

Bei Mac-Benutzern treten bei der CLI-Authentifizierung für interne Anwendungen während der Verbindung mit Cisco Secure Client VPN gelegentlich Fehler auf. Die Fehler treten während der CLI-Authentifizierung und bei der Verwendung von Befehlen wie `curl` als "host not found"-Fehler auf. Die DNS-Auflösungsbefehle wie `nslookup` und `dig` sind jedoch erfolgreich. Das Problem tritt willkürlich auf und kann vorübergehend gelöst werden, indem das VPN erneut verbunden wird. Zeitraum, bevor das Problem erneut auftritt. Split-tunnel VPN wird verwendet, und Cisco Umbrella ist aktiv. Das Problem tritt nicht auf, wenn Palo Alto GlobalProtect VPN verwendet wird.

- Fehlermeldung: "host not found" (Host nicht gefunden) für CLI-Authentifizierung und `Curl`-Befehle
- Fehlermeldung: Der VPN-Client kann die Änderungen der IP-Weiterleitungstabelle nicht erfolgreich überprüfen. DNS-Auflösungsproblem beim Verbinden privater Ressourcen
- `nslookup`- und `dig`-Befehle erfolgreich
- Intermittierende Verbindungen nach der erneuten Verbindung mit VPN
- Remote-Access-VPN mit Split-Tunnel und aktiviertes Umbrella-Modul
- Problem nur mit Cisco Secure Client VPN auf MacOS-Geräten reproduzierbar

Umwelt

- Produkt: Cisco Secure Client (CSC) mit mehreren Modulen
- Plattform: Mac-Geräte für Unternehmen
- VPN-Profilkonfiguration: VPN-Profil für den Remote-Zugriff - Umgehung des sicheren Zugriffs - Split-Tunnel-Modus und DNS-Modus als "Standard-DNS" ausgewählt
- DNS-Filterung: Cisco Umbrella aktiviert
- Modulversionen:
    - Cloud-Management v1.0.0.23
    - AnyConnect VPN v5.1.13.177
    - Umbrella v5.1.13.177
    - DART v5.1.13.177
    - Secure Firewall Status v5.1.13.177

    - Network Visibility-Modul v5.1.13.177
- Diagnosedaten: Zur Analyse gesammelte DART-Pakete
- Nur bei Cisco Secure Client VPN (nicht bei Palo Alto GlobalProtect) beobachtet

Auflösung

- Beim Debuggen der VPN-Profilkonfiguration (`naic.org`) und der Client-seitigen AnyConnect VPN-Routing-Tabelle wurde dieses Verhalten beobachtet:
    - Arbeitsszenario - Bei einer `nslookup`-Suche für die lokalen Domänen des Tresors, die keine Produkte sind, wurden die DNS-Anfragen, die von den im VPN-Profil konfigurierten DNS-Servern verarbeitet wurden, korrekt in 10.x-Adressen aufgelöst. Entsprechend wurde die Routing-Tabelle mit der aufgelösten IP (z. B. 10.59.130.193) unter nicht sicheren Routen aktualisiert.
    - Nicht funktionierendes Szenario - Wenn dieselben DNS-Anfragen jedoch vom lokalen DNS (192.168.x.x) des macOS-Systems verarbeitet wurden, der auf den Adaptern untun4 und en0 konfiguriert wurde, anstatt auf den im VPN-Profil definierten DNS-Servern, wurde dieses Verhalten bei der Paketerfassung deutlich beobachtet, während das Problem festgestellt wurde.
    - Die privaten Domänen haben sich in den IP-Bereich 34.x.x.x aufgelöst, was zu dem Verbindungsproblem geführt hat. Die Erfassung von Wireshark half dabei, diese zugrunde liegende Ursache des Problems zu identifizieren.
- Im Hinblick auf Design und Konfiguration wird bei der Einrichtung eines VPN-Profils für Split-Tunnel die Verwendung von Split-DNS empfohlen, anstatt sich auf das lokale System DNS/Standard-DNS zu verlassen.
- Außerdem wurde der Eintrag `us-east-eks-amazonaws.com` hinzugefügt, um sicherzustellen, dass der Datenverkehr für diesen EKS-Cluster korrekt durch die Remote-Tunnelschnittstelle geleitet wird.
- Ebenfalls diskutiert wurde, dass die RAVPN-Schnittstelle Vorrang vor dem Umbrella-Modul haben muss und nicht mit der Datei `OrgInfo.json` kollidieren darf, die die Umbrella Organization ID enthält.
- Während unserer Fehlerbehebung haben wir eine Neuinstallation des CSC-Clients ohne Umbrella-Modul durchgeführt, mit diesem Szenario konnten wir das Problem nicht sehen. Ich konnte auch aus Umbrella-Perspektive überprüfen, Root-Domain naic.org in der internen Domains-Liste konfiguriert, um Umbrella zu umgehen, was bedeutet, dass lokale Domain-Auflösungen an macOS konfigurierte System-DNS weitergeleitet wird nicht durch Umbrella DNS-Modul auf Kernel-Ebene Loopback abgefangen Schnittstelle.

Dies entspricht der Problembehebung, wenn kein Umbrella-Modul vorhanden ist. Mit der richtigen VPN-Profilkonfiguration, einschließlich der richtigen Domänen in der Verkehrssteuerungsregel und der geteilten DNS-Konfiguration, sollte das Problem nicht angezeigt werden, auch wenn das Umbrella-Modell EIN ist.

Der Benutzer bestätigte, dass das Problem behoben wurde, nachdem er den DNS-Modus auf Split Tunnel geändert und die VPN-Profilkonfiguration bearbeitet hatte.

Ursache

VPN-Profil - Sicheren Zugriff umgehen - Der DNS-Modus sollte auf "Split Tunnel" gesetzt werden (am häufigsten verwendete Optionen in Anwendungsfällen) und alle privaten/internen Anwendungsdomänen in die Split DNS-Konfiguration einschließen, um das Problem zu beheben.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

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.