Cisco Secure Access RAVPN Protocol - Verhalten mit TLS/DTLS und IPsec(IKEv2) Dual-Konfiguration

Inhalt

Problem

Wenn TLS/DTLS- und IPsec(IKEv2)-Protokolle in Cisco Secure Access RAVPN aktiviert sind und das primäre Protokoll auf IPsec(IKEv2) gesetzt ist, treten beim Versuch, VPN-Verbindungen von Netzwerken herzustellen, in denen IPsec-Datenverkehr (UDP-Ports 500/4500) blockiert ist, Verbindungsfehler auf. Der Secure Client verwendet standardmäßig die IPsec-Option in der Dropdown-Liste mit der Client-Benutzeroberfläche und führt kein automatisches Failover auf TLS/DTLS aus, wenn die IPsec-Verbindung ausfällt. Dies führt zu Verbindungsfehlern und verhindert die Einrichtung einer RAVPN-Verbindung aus eingeschränkten Netzwerkumgebungen.

Umwelt

- Cisco Secure Access RAVPN mit Dual Protocol-Konfiguration
- TLS/DTLS- und IPsec(IKEv2)-Protokolle aktiviert
- Primäre Protokolleinstellung konfiguriert als IPsec(IKEv2)
- Secure Client mit Protokoll-Auswahl-Dropdown-Liste, die separate IPsec- und TLS-Optionen enthält
- Netzwerkumgebung blockiert IPsec-Datenverkehr an den UDP-Ports 500 und 4500

Auflösung

Das beobachtete Verhalten wird erwartet und ist geplant. Cisco Secure Access RAVPN führt kein automatisches Protokoll-Failover von IPsec (IKEv2) zu TLS/DTLS durch, wenn beide Protokolle aktiviert sind und das primäre Protokoll Verbindungsprobleme feststellt.

Manuelle Protokollauswahl erforderlich

Wenn Benutzer eine Verbindung von Netzwerken herstellen, die IPsec-Datenverkehr blockieren, müssen sie das entsprechende Protokoll manuell in Secure Client auswählen:

Schritt 1: Öffnen Sie die Anwendung Secure Client.

Phase 2: Suchen Sie in der Client-Schnittstelle nach dem Dropdown-Menü für die Protokollauswahl.

Schritt 3: Ändern Sie die Auswahl manuell von der IPsec-Option in die TLS-Option.

Schritt 4: VPN-Verbindung mit TLS/DTLS-Protokoll initiieren

Klärung des Protokollverhaltens

Die Einstellung für das primäre Protokoll in Cisco Secure Access RAVPN legt das Standardprotokoll im Secure Client fest, aktiviert jedoch keine automatische Failover-Funktion. Wenn TLS/DTLS und IPsec(IKEv2) aktiviert sind:

- Der Secure Client zeigt im Dropdown-Menü separate Protokolloptionen an
- Der Client verwendet standardmäßig die Einstellung für das primäre Protokoll (in diesem Fall IPsec).
- Basierend auf Netzwerkverbindungsbedingungen erfolgt kein automatisches Switching zwischen Protokollen.
- Benutzer müssen das entsprechende Protokoll basierend auf ihrer Netzwerkumgebung manuell auswählen.

Ursache

Cisco Secure Access RAVPN wurde ohne automatische Protokoll-Failover-Funktion konzipiert. Wenn die Protokolle TLS/DTLS und IPsec(IKEv2) aktiviert sind, muss das Protokoll über die Secure Client-Schnittstelle manuell ausgewählt werden. Die Einstellung für das primäre Protokoll legt nur die Standardauswahl im Client-Dropdown-Menü fest und implementiert keine automatische Switching-Logik, wenn Verbindungsprobleme mit dem primären Protokoll auftreten.

Verwandte Inhalte

- Cisco Secure Access-Dokumentation
- 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.