Sicherer Zugriff Split-Tunneling-Konfigurationsherausforderungen

Inhalt

Problem

Bei der Konfiguration der Cisco Secure Access (TIA)-Funktion für Split-Tunnel-Datenverkehr traten während des Konfigurationsprozesses mehrere Komplikationen auf, die eine ordnungsgemäße Bereitstellung verhinderten:

- Probleme bei der Identifizierung des Datenverkehrs: Bei der Konfiguration von TIA für Split-Tunneling muss der gesamte VPN-Verkehr aus der Internet-Sicherheitsprüfung ausgeschlossen werden. Die Identifizierung der erforderlichen Datenverkehrsflüsse erwies sich als schwierig, und einige URLs für die Umleitung waren besonders schwierig zu verfolgen und zu kategorisieren.
- Einschränkungen für den Authentifizierungsverkehr: Bei bestimmten Split-Tunnel-Szenarien musste der Authentifizierungsverkehr vom Proxy ausgeschlossen werden. Auf der Grundlage der vorhandenen Richtlinien konnte der authentifizierungsbezogene Datenverkehr jedoch nicht vom Proxy umgangen werden, was zu Richtlinienkonflikten führte.
- Sicherheitsrisiken bei VPN-Trennung: Der Split-Tunnel-Datenverkehr wird dem offenen Internet ausgesetzt, wenn die VPN-Verbindung getrennt wird. Dies führt zu zusätzlichen Sicherheitsrisiken, die bei der Konfiguration berücksichtigt werden müssen.

Während des Prozesses traten außerdem weitere Konfigurationsprobleme auf, die einer weiteren Analyse und Behebung bedurften.

Umwelt

- Produktfamilie: SECACCS (sicherer Zugriff)
- Technologie: Cisco Secure Access (TIA) mit Split-Tunneling-Funktion

- Konfiguration: Szenarien mit getrenntem Tunnelverkehr und vorhandenen Richtlinien
- Authentifizierung: Proxy-basierte Verarbeitung von Authentifizierungsdatenverkehr
- Netzwerksicherheit: Anforderungen für die Internet-Sicherheitsüberprüfung des VPN-Datenverkehrs

Auflösung

Basierend auf den Konfigurationsherausforderungen im Zusammenhang mit Cisco Secure Access Split-Tunneling wurde eine Anforderung für umfassende Funktionen eingereicht, um die ermittelten Einschränkungen und Richtlinienkonflikte zu beheben.

Einsendung der Funktionsanforderung

Eine Funktionsanfrage (CSE-I-5636) wurde geöffnet und dem zuständigen Technikerteam zur Prüfung vorgelegt, um die folgenden Konfigurationsherausforderungen zu erfüllen:

- Verbesserte Identifizierungsfunktionen für den VPN-Datenverkehr, um ihn von der Internet-Sicherheitsüberprüfung auszunehmen
- Verbesserte Handhabung von schwer zu verfolgenden und zu kategorisierenden Umleitungs-URLs
- Behebung von Einschränkungen bei der Umgehung des Authentifizierungsdatenverkehrs durch bestehende Richtlinien
- Minderung von Sicherheitsrisiken für Split-Tunnel-Datenverkehr während der VPN-Trennung

Ursache

Die Probleme bei der Konfiguration ergeben sich aus den aktuellen Einschränkungen der Cisco Secure Access (TIA) Split-Tunneling-Implementierung, die komplexe Bereitstellungsszenarien in Unternehmen nicht ausreichend berücksichtigen. Das System bietet keine ausreichende präzise Kontrolle für die Identifizierung und Kategorisierung von Datenverkehr, es unterliegt gewissen Einschränkungen bei der Umgehung von Authentifizierungsdatenverkehr, wenn Richtlinien

vorhanden sind, und es bietet keine ausreichenden Sicherheitsmechanismen für Split-Tunnel-Datenverkehr, wenn VPN-Verbindungen unterbrochen werden.

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.