DNS-Protokollierung und Geräteregistrierungsverhalten mit Cisco Secure Client auf iOS für Remote Access VPN

Inhalt

Problem

Bei der Verwendung von Cisco Secure Client auf iOS (iPad) zur Einrichtung eines Remote Access VPN mit Cisco Secure Access mithilfe der SAML-Authentifizierung über Microsoft Entra ID werden DNS-Protokolle nach erfolgreicher VPN-Verbindung nicht in Secure Access angezeigt, obwohl Firewall- und Webprotokolle korrekt generiert wurden. Außerdem wird das iPad nach Einrichtung der VPN-Verbindung nicht unter Roaming Devices (Roaming-Geräte) > Mobile Devices (Mobile Geräte) im Dashboard für sicheren Zugriff angezeigt.

Zu den beobachteten spezifischen Symptomen gehören:

- Remotezugriffsprotokolle zeigen erfolgreiche "connect"-Ereignisse in sicherem Zugriff an
- Es werden Firewall- und Webprotokolle generiert, die die SAML-authentifizierte Benutzeridentität anzeigen.
- DNS-Protokolle sind in der Protokollierung für sicheren Zugriff nicht vorhanden.
- Die iPad-Geräteinformationen werden nicht im Abschnitt "Roaming-Geräte für sicheren Zugriff" ausgefüllt.
- Der gesamte Datenverkehr fließt durch den VPN-Tunnel (kein Split-Tunneling konfiguriert).

Umwelt

- iPad mit iOS 26.2
- Cisco Secure Client

- Identitätsanbieter: Microsoft Entra-ID
- Sicherheitsanschluss: Nicht installiert
- Cisco Secure Access mit konfigurierter SSO-Authentifizierung
- Implementierung der SAML-Authentifizierung
- VPN-Profil, für das der DNS-Modus standardmäßig konfiguriert ist
- Kein Split-Tunneling konfiguriert (der gesamte Datenverkehr wird über VPN geleitet)
- Mobile Device Management (MDM) für die Profilverteilung

Auflösung

Das beobachtete Verhalten wird für die dokumentierte Konfiguration erwartet. Der Cisco Secure Client unter iOS fungiert als VPN-Client (entspricht AnyConnect) und bietet standardmäßig keine RSM-äquivalente Funktionalität. Security Connector ist die RSM-äquivalente Komponente in iOS für die Population der Endgeräteidentität und die Umbrella-artige DNS-Kontrolle.

Die Architektur

Das Fehlen von DNS-Protokollen und der Geräteregistrierung tritt aus folgenden Gründen auf:

- Cisco Secure Client allein bietet VPN-Verbindungen, jedoch keine für die DNS-Transparenz erforderlichen Endpunkt-Agent-Funktionen
- Security Connector (entspricht RSM unter Windows) ist für die DNS-Steuerung und die Geräteregistrierung in Secure Access erforderlich.
- Ohne Security Connector werden DNS-Abfragen von den VPN-DNS-Servern ohne Transparenz für Umbrella/Secure Access verarbeitet.

DNS-Protokollierungslösung über Verkehrssteuerung

Um die DNS-Protokollierung ohne Installation von Security Connector zu aktivieren, konfigurieren

Sie die Datenverkehrssteuerung, um DNS-Abfragen an Umbrella DNS-Server weiterzuleiten:

Schritt 1: Konfigurieren der Datenverkehrssteuerung in sicherem Zugriff

Navigieren Sie zu Traffic Steering > Add > Add a source, und geben Sie die IP-Adresse des DNS-Servers als Quelle an.

Phase 2: Direkter DNS-Datenverkehr zu Umbrella Servern

Konfigurieren Sie das VPN-Profil zur Verwendung von Umbrella DNS-Servern (208.67.222.222 und 208.67.220.220), um sicherzustellen, dass DNS-Abfragen für den sicheren Zugriff sichtbar sind.

Schritt 3: DNS-Protokollierung überprüfen

Nach der Implementierung der Konfiguration der Datenverkehrssteuerung sollten DNS-Protokolle im Secure Access Dashboard für VPN-Sitzungen angezeigt werden.

DNS-Moduseinstellung für VPN-Profil

Die Einstellung "DNS Mode" (DNS-Modus) im VPN-Profil hat keinen Bezug zum Fehlen von DNS-Protokollen in dieser Konfiguration. Bei RAVPN-Sitzungen (Remote Access VPN) werden unabhängig von dieser Einstellung die VPN-bezogenen DNS-Server verwendet. Die Transparenz der Protokollierung hängt davon ab, ob der DNS-Verkehr an die überwachte DNS-Infrastruktur weitergeleitet wird.

Installationsoption für Security Connector

Die Installation von Security Connector unter iOS ermöglicht Folgendes:

- Transparenz der DNS-Protokollierung für sicheren Zugriff
- Verbesserte Endgeräteidentität und Funktionen zur Geräteregistrierung
- Umbrella-Style DNS-Steuerung und -Schutz

Der Security Connector kann in Verbindung mit dem Secure Client verwendet werden. Um Konflikte zwischen den beiden Komponenten zu vermeiden, müssen jedoch der Datenverkehr ausgeschlossen und das Design entsprechend angepasst werden.

Ursache

Die Ursache liegt in der Architektur: Cisco Secure Client auf iOS bietet VPN-Verbindungen, bietet jedoch nicht die für die DNS-Transparenz und die Geräteregistrierung in Secure Access erforderlichen Endpunkt-Agent-Funktionen. Für diese Funktion ist entweder die Installation des Security Connectors oder die Konfiguration der Datenverkehrssteuerung erforderlich, um DNS-Abfragen über die überwachte Infrastruktur zu leiten. Ohne diese Komponenten umgehen DNS-Abfragen die Überwachung des sicheren Zugriffs, und die Informationen zur Geräteidentität werden nicht in den Abschnitt für Roaming-Geräte eingefügt.

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.