Verbindungsfehler beim Azure VPN-Client mit aktivierter Websicherheit für sicheren Zugriff

Inhalt

Problem

Nach der Migration von Umbrella zu SSE und der Aktivierung von Web Security mit einer neu zugewiesenen SIA-Lizenz können Azure VPN Client-Verbindungen für Benutzer nicht hergestellt werden, wenn Web Security aktiviert ist. Das Verbindungsproblem bei Azure VPN-Clients wirkt sich auf alle Clients aus und verhindert, dass diese sich mit dem VPN verbinden. Wenn der Cisco Secure Access-Client von Clientcomputern deinstalliert wird, wird die VPN-Verbindung wiederhergestellt. Dies weist darauf hin, dass der Secure Access-Client die Verbindung zu Azure VPN-Diensten blockiert.

Wenn Sie die Websicherheit deaktivieren oder den Cisco Secure Access Client deinstallieren, wird die VPN-Verbindung wiederhergestellt. Dies wirkt sich jedoch auf den Benutzerzugriff auf Ressourcen über Azure VPN aus, wenn ein Websicherheitsschutz erforderlich ist.

Umwelt

- Cisco Secure Access (ehemals SIA) mit aktivierter Websicherheit
- Azure-VPN-Client
- Migration von Umbrella zu SSE abgeschlossen
- Neu zugeordnete SIA-Lizenz

Auflösung

Die Auflösung beinhaltet das Hinzufügen der öffentlichen IP-Adresse des Azure VPN-Gateways

zur SSE/SWG-Ausnahmeliste, um ein Abfangen des Datenverkehrs zu verhindern, das VPN-Verbindungen blockiert.

Schritt 1: Identifizieren der IP-Adresse des Azure VPN-Gateways

Bestimmen Sie die öffentliche IP-Adresse des Azure VPN-Gateways.

Phase 2: IP-basierte Ausnahme zu SSE/SWG hinzufügen

1.- Fügen Sie die öffentliche Azure Virtual Gateway-IP-Adresse der SSE/SWG-Ausnahmeliste in der Cisco Secure Access-Umgebung hinzu.

2.- Melden Sie sich beim Cisco Secure Access Dashboard an. Klicken Sie auf Verbinden - Endbenutzerverbindung - Internetsicherheit - Ausnahme hinzufügen. Dadurch wird verhindert, dass das sichere Web-Gateway den Datenverkehr abfangen und überprüfen kann, der für das Azure VPN-Gateway bestimmt ist.

Schritt 3: VPN-Verbindungen testen

Testen Sie nach der Anwendung der IP-basierten Ausnahme die Azure VPN-Verbindung, um sicherzustellen, dass die Clients erfolgreich VPN-Verbindungen mit aktivierter Websicherheit herstellen können.

Schritt 4: Erweitern Tests

Testen Sie die IP-basierte Ausnahme auf weitere Benutzer in der gesamten Umgebung, um eine konsistente Funktionalität sicherzustellen, bevor Sie die Lösung als abgeschlossen betrachten.

Ursache

Das Problem tritt auf, weil der Ausnahmemechanismus des sicheren Webgateways (SWG) eine DNS-Suche für eine Domäne erfordert, um einen Eintrag im Cache von Domäne zu IP zu erstellen. Wenn der Azure VPN-Client eine direkte Verbindung mit der IP-Adresse herstellt, ohne eine DNS-Abfrage für die VPN-URL durchzuführen, kann das SWG-Modul die Domäne nicht der IP-Adresse zuordnen. Die SWG untersuchen daher weiterhin den an die IP-Adresse gesendeten Datenverkehr und halten ihn ab, sodass keine VPN-Verbindung hergestellt werden kann.

Die Paketerfassungsanalyse zeigte keine DNS-Abfragen für die VPN-URL und keinen sichtbaren SWG-Interception-Datenverkehr für die Azure-Gateway-IP-Adresse. Dies bestätigte, dass die SWG die Verbindung blockierte, da im Cache keine ordnungsgemäße Zuordnung von Domäne zu IP vorhanden war.

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.