Popup-Fenster "Secure Client Machine Tunnel Authentication" löst Verbindungen in nicht vertrauenswürdigen Netzwerken aus

Inhalt

Problem

Cisco Secure Client (AnyConnect) fordert Benutzer wiederholt zur Eingabe von Benutzername und Kennwort auf, während ein Maschinentunnel verbunden ist, insbesondere wenn Benutzer Verbindungen über nicht vertrauenswürdige Netzwerke herstellen. Das Authentifizierungs-Popup unterbricht die Verbindung mit dem Maschinentunnel und verursacht Verbindungsunterbrechungen, was sich auf die Fähigkeit der Benutzer auswirkt, einen stabilen Remote-Zugriff aufrechtzuerhalten. Dieses Problem tritt auf, obwohl der Maschinentunnel ordnungsgemäß eingerichtet und authentifiziert wurde. Das Popup wird unerwartet angezeigt, und die VPN-Sitzungskontinuität wird unterbrochen.

Umwelt

- Cisco Secure Client (AnyConnect) mit Maschinentunnel-Konfiguration
- VPN-Profil für Remote-Zugriff mit aktivierter Trust Network Detection (TND)-Funktion
- Benutzercomputer mit Maschinentunnel verbunden
- Gruppenrichtlinienobjekte (Group Policy Objects, GPO) für die Verteilung von Clientprofilen
- Sowohl Benutzer-Tunnel- als auch Maschinen-Tunnelprofile, die mit TND-Einstellungen konfiguriert wurden

Auflösung

Das Problem wurde durch die Änderung der TND-Konfigurationseinstellungen (Trust Network Detection) sowohl für das System- als auch für das Benutzertunnelprofil behoben. Die Lösung umfasst die Konfiguration des TND-Aktionverhaltens, um unnötige Authentifizierungsaufforderungen in nicht vertrauenswürdigen Netzwerken zu vermeiden.

Schritt 1: Konfigurieren der TND-Einstellungen für nicht vertrauenswürdige Netzwerke

Legen Sie die Aktion "Netzwerkerkennung vertrauen" auf "Keine Aktion für nicht vertrauenswürdige Netzwerke in Computertunneln und Benutzertunnelprofilen" fest. Durch diese Konfiguration wird verhindert, dass der Client beim Herstellen einer Verbindung mit nicht vertrauenswürdigen Netzwerken zur Eingabe zusätzlicher Anmeldeinformationen auffordert.

Phase 2: Konfigurieren der TND-Einstellungen für vertrauenswürdige Netzwerke

Setzen Sie die Aktion "Netzwerkerkennung vertrauen" auf Verbindung für vertrauenswürdige Netzwerke trennen, um das beabsichtigte Sicherheitsverhalten für bekannte sichere Netzwerkumgebungen aufrechtzuerhalten.

Schritt 3: Bereitstellen von Konfigurationsänderungen

Stellen Sie die aktualisierten TND-Einstellungen per Gruppenrichtlinienobjekt-Push bereit, um die Konfigurationsänderungen auf alle betroffenen Client-Computer zu verteilen.

Schritt 4: Neustart der Client-Computer

Starten Sie die Client-Computer nach der Profilaktualisierung neu, um sicherzustellen, dass die neuen TND-Einstellungen ordnungsgemäß wirksam werden.

Schritt 5: Validierungstests

Testen Sie die Verbindung des Maschinentunnels über mehrere nicht vertrauenswürdige Netzwerke hinweg, um sicherzustellen, dass:

- Das Authentifizierungs-Popup wird nicht mehr angezeigt.
- Maschinentunnel bleibt durchgängig verbunden
- Keine Anmeldeinformationen fordern Unterbrechung der VPN-Sitzung
- Benutzer können einen stabilen Remote-Zugriff ohne Verbindungsunterbrechung aufrechterhalten

Der Benutzer bestätigte die erfolgreiche Problembehebung nach der Implementierung dieser Änderungen. Mehrere Benutzertests validierten die Kontinuität stabiler VPN-Sitzungen über verschiedene Netzwerkbedingungen hinweg.

Ursache

Die Ursache dafür waren falsch konfigurierte Trust Network Detection (TND)-Einstellungen in den Cisco Secure Client-Profilen. Die TND-Funktion löste Authentifizierungsaufforderungen aus, wenn Benutzer eine Verbindung über nicht vertrauenswürdige Netzwerke herstellen, obwohl der Maschinentunnel bereits ordnungsgemäß authentifiziert und eingerichtet wurde. Die TND-Aktionen für Benutzer- und Maschinentunnelprofile waren nicht optimal für die Netzwerkumgebung konfiguriert, sodass der Client unnötigerweise zusätzliche Anmeldedaten anfordert und die Verbindung zum Maschinentunnel unterbrochen wird.

Verwandte Inhalte

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.