

Secure Client TND - Überlegungen zum manuellen VPN-Verbindungsverhalten und zur URL-Sperrung

Inhalt

Problem

Bei Verwendung eines VPN-Profiles mit der Funktion zur Erkennung vertrauenswürdiger Netzwerke (Trusted Network Detection, TND), die mit der Einstellung für vertrauenswürdiges Netzwerk auf "Trennen" konfiguriert wurde, können Endpunkte innerhalb des vertrauenswürdigen Netzwerks weiterhin erfolgreich eine VPN-Verbindung herstellen, wenn Benutzer manuell Verbindungen über den Cisco Secure Client initiieren.

Dieses Verhalten tritt auf, obwohl die TND-Konfiguration so eingestellt ist, dass VPN-Sitzungen getrennt werden, wenn der Endpunkt in einem vertrauenswürdigen Netzwerk erkannt wird.

Zu den ermittelten spezifischen Bedenken gehören:

- Manuelle VPN-Verbindungen von Trusted Network-Endpunkten können nicht über die Standard-TND-Konfiguration gesteuert oder blockiert werden
- Unsicherheit, ob die Cisco Secure Access (CSA)-Einstellungen manuelle VPN-Verbindungen von vertrauenswürdigen Netzwerkendpunkten blockieren können
- Fragen zur Stabilität der VPN-Profilverbindungs-URL (xxxx.vpn.sse.cisco.com) und ob sich diese regelmäßig ändert, was sich auf Firewall-basierte Blockierungsstrategien auswirken kann

Umwelt

- Cisco Secure Access (CSA)-Bereitstellung
- Cisco Secure Client mit VPN-Profilkonfiguration

- Trusted Network Detection (TND)-Funktion aktiviert
- Einstellung für vertrauenswürdiges TND-Netzwerk als "Verbindung trennen" konfiguriert
- Endpunkte im konfigurierten vertrauenswürdigen Netzwerk
- Firewall-Infrastruktur für Netzwerkzugriffskontrolle

Auflösung

Verständnis des TND-Verhaltens durch manuelle VPN-Verbindungen

Das beobachtete Verhalten stimmt mit der dokumentierten Cisco Secure Client-Funktion überein. Laut Cisco-Dokumentation trennt oder verhindert TND keine VPN-Sitzung, die ein Benutzer manuell startet, während er sich in einem vertrauenswürdigen Netzwerk befindet. Dies ist das erwartete Verhalten, unabhängig von den TND-Konfigurationseinstellungen.

Die wichtigsten technischen Fakten sind:

- Die Funktion zur automatischen Trennung von TNDs gilt nur für automatisch hergestellte VPN-Verbindungen.
- Manuelle VPN-Verbindungen, die von Benutzern initiiert werden, umgehen das TND-Trennungsverhalten.
- Es ist keine CSA-Konfigurationseinstellung zum Blockieren manueller VPN-Verbindungen von vertrauenswürdigen Netzwerkendpunkten vorhanden.

Strategie zur betrieblichen Risikominimierung

Die primäre Methode zur Kontrolle manueller VPN-Verbindungen von Trusted Network-Endpunkten aus besteht in der Kontrolle auf Netzwerkebene:

Schritt 1: Firewall-URL-Blockierung implementieren: Konfigurieren Sie die Trusted Network Firewall so, dass der Zugriff auf die VPN-Profilverbindungs-URL (xxxx.vpn.sse.cisco.com) blockiert wird. Dadurch wird verhindert, dass Endpunkte im vertrauenswürdigen Netzwerk den

Endpunkt des VPN-Service erreichen.

Phase 2: Überprüfung der URL-Stabilität: Die VPN-Profil-URL-ID (der xxxx-Teil) ist tenant-spezifisch und wird voraussichtlich nicht regelmäßig geändert. Dadurch wird ein stabiles Ziel für Firewall-Blockierungsregeln bereitgestellt.

Validierung und Tests

Die Tests haben bestätigt, dass das Blockieren der VPN-Profilverbindungs-URL an der Firewall des vertrauenswürdigen Netzwerks Endpunkte erfolgreich daran hindert, VPN-Verbindungen herzustellen, selbst wenn Benutzer versuchen, manuelle Verbindungen über den Cisco Secure Client herzustellen.

Ursache

Dieses Verhalten wird in der Cisco Secure Client TND-Implementierung festgelegt. Die TND-Funktion wurde speziell für die Verwaltung automatischer VPN-Verbindungen basierend auf dem Status der Netzwerkvertrauenswürdigkeit entwickelt. Manuelle VPN-Verbindungen, die vom Benutzer initiiert wurden, werden dadurch jedoch nicht beeinträchtigt. Dieses Design ermöglicht Benutzern, bei Bedarf automatisches Verhalten außer Kraft zu setzen und bietet gleichzeitig eine automatische Netzwerkerkennung und ein automatisches Verbindungsmanagement für typische Anwendungsfälle.

Verwandte Inhalte

- [Administratoranleitung für Cisco Secure Client - TND-Konfiguration](#)
- [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.