

Methoden der sicheren Client-Verteilung für RAVPN mit sicherem Zugriff

Inhalt

Problem

Bei der Konfiguration des Zugriffs externer Anbieter auf Remote Access VPN (RAVPN) in Cisco Secure Access benötigen Administratoren eine Methode, mit der Anbieter die AnyConnect/Secure Client-Software herunterladen können. Im Gegensatz zu früheren ASA-Bereitstellungen, bei denen die VPN-URL für direkte Client-Downloads bereitgestellt wurde, bieten die Cisco Secure Access VPN-Headend-URLs keine Client-Download-Funktion. Diese Einschränkung wirkt sich auf den Onboarding-Prozess für externe Anbieter aus, die Remote-Zugriff benötigen.

Die Administratoren erwarten, dass die VPN-Setup-URLs in Secure Access den Anbietern Zugriff zum Herunterladen des AnyConnect-Clients gewähren. Dies entspricht in etwa dem zuvor bei ASA-basierten Bereitstellungen verfügbaren Verhalten, bei dem die VPN-URL Client-Downloads vor dem Herstellen der Verbindung zulässt.

Umwelt

- Cisco Secure Access mit RAVPN-Konfiguration
- Externe Zugriffsanforderungen für Anbieter
- Migration von einer ASA-basierten VPN-Bereitstellung
- Verteilungsanforderungen für AnyConnect/Secure Client

Auflösung

Cisco Secure Access hostet keine Secure Client-Pakete auf den VPN-Headend-URLs. Die

Lösung verwendet Hostscan-Technologie, anstatt direkte Client-Downloads über die VPN-URL bereitzustellen. Um die Secure Client-Software an externe Anbieter zu verteilen, verwenden Sie eine der folgenden genehmigten Methoden.

Methode 1: Dashboard-Verteilung für sicheren Zugriff

1.- Rufen Sie Installationspakete direkt vom Secure Access Dashboard zur manuellen Verteilung ab.

2.- Navigieren Sie zu Endbenutzerverbindungen, und klicken Sie auf die Schaltfläche Cisco Secure Client, um Installationspakete zur Verteilung an Anbieter herunterzuladen.

Methode 2: Cisco Software-Download-Site

Anbieter können Pakete direkt herunterladen, wenn sie über die richtigen Berechtigungen verfügen:

- Der Anbieter muss über ein Cisco Konto mit Softwareberechtigung verfügen.
- Rufen Sie die Pakete unter software.cisco.com auf.
- Erfordert eine vor der Bereitstellung durchzuführende Planung und Einrichtung von Cisco Anbieterkonten

Methode 3: Manuelle Verteilung

Die Secure Client-Software kann manuell oder über alternative Vertriebskanäle außerhalb der VPN-URL an externe Anbieter verteilt werden. Diese Methode bietet die größte Kontrolle über den Verteilungsprozess und erfordert keine Cisco-Kreditorenkonten.

Ursache

Die URLs für das VPN-Headend von Cisco Secure Access unterscheiden sich von den ASA-basierten Bereitstellungen. Die Secure Access-Lösung hostet keine Client-Installationspakete auf den Headends und verwendet stattdessen die Host-Scan-Technologie. Aufgrund dieser unterschiedlichen Architektur können die VPN-URLs nicht dieselbe Client-Downloadfunktionalität bieten, die bei ASA-Bereitstellungen verfügbar 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.