RAVPN-Verbindung für Remote-Zugriffsbenutzer mit internen Services nicht möglich

Inhalt

Problem

Benutzer von Remote-Zugriff, die Secure Access verwenden, konnten keine internen Services erreichen, einschließlich des Domänencontrollers in der Zentrale. Der Internetzugriff funktionierte hingegen normal. Benutzer konnten erfolgreich im Internet surfen, aber nicht auf interne Ressourcen wie den Domänencontroller über RAVPN (Remote Access VPN) zugreifen.

Umwelt

- Cisco Secure Access - Sicherer Client-Remote-Zugriff (VPN, Status, private Ressource)
- RAVPN-Tunnel (Remote Access VPN) werden als aktiv und fehlerfrei gemeldet
- SD-WAN-Infrastruktur in Betrieb
- Interne DNS-Server in der Zentrale
- Domain Controller-Services am Hauptsitz
- Mehrere Zweigstellennetzwerke, die über die Infrastruktur verbunden sind

Auflösung

Die folgenden Schritte zur Fehlerbehebung und Problembehebung wurden durchgeführt, um das Problem der RAS-Verbindung zu beheben:

Schritt 1: Paketerfassungsanalyse

Sammeln Sie die simultane Paketerfassung vom Client und Ihrem Edge-Gerät (bidirektional), um Datenflussmuster zu analysieren.

Fluss:

RA VPN-Client ----------Cisco Secure Access --------IPSec-Tunnel ---------- Edge-Gerät --------- Private Ressource

- Bestätigen Sie, ob DNS-Abfragen von Clients das Edge-Gerät erreicht haben und an den DNS-Server gesendet werden sollen.
- Überprüfen Sie, ob keine DNS-Antworten vom lokalen DNS-Server zu den Clients zurückgesendet wurden.
- Der lokale DNS-Server hat eine Antwort gesendet, die jedoch nie an die Tunnelschnittstelle zurückgesendet wurde.

Phase 2: Ursachenidentifizierung

Basierend auf der Paketerfassungsanalyse wurde das Problem als ein Problem mit der Rückpfad-Weiterleitung erkannt. Die Datenverkehrsanalyse ergab, dass DNS-Abfragen den lokalen DNS-Server zwar erfolgreich über die Cisco Secure Access-Infrastruktur erreichten, der zurückgesendete Datenverkehr mit DNS-Antworten jedoch aufgrund von Routing- oder Konfigurationsproblemen in der Infrastruktur nicht die Remote Access-Clients erreichte.

Schritt 3: Überprüfung der Konfiguration und Problembehebung

Überprüfen und korrigieren Sie die interne Netzwerkkonfiguration und die interne Netzwerkkonfiguration. Konzentrieren Sie sich dabei auf folgende Punkte:

- DNS-Konfiguration und Routing des zurückkehrenden Datenverkehrs
- Interne Routing-Richtlinien für VPN-Rückverkehr
- Interne Netzwerk-Routing-Konfiguration

- Fehlende Konfigurationselemente auf Seite des Edge-Geräts

Schritt 4: Überprüfung der Servicewiederherstellung

Nach der Konfigurationsprüfung und Korrekturen wurde die Funktion für sicheren Zugriff größtenteils wiederhergestellt. Die meisten Remote Access-Benutzer haben wieder Zugriff auf interne Services, einschließlich des Domänencontrollers in der Zentrale.

Ursache

Die Ursache wurde als ein Problem mit dem Routing des Rückpfad innerhalb der internen Netzwerkinfrastruktur identifiziert. Während DNS-Abfragen von RAS-Clients erfolgreich den lokalen DNS-Server über die Cisco Secure Access-Infrastruktur erreichten, wurde der zurückgesendete Datenverkehr mit DNS-Antworten nicht ordnungsgemäß an die Clients zurückgeleitet. Dies wurde durch fehlende oder falsche Konfiguration auf der Seite der internen Netzwerkinfrastruktur verursacht, die verhindert hat, dass DNS-Antworten und TCP-Antworten die RAS-Clients über die VPN-Verbindung erreichen.

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.