

Probleme mit der Datensatzauflösung für Jabber DNS SRV mit Cisco Secure Access VPN

Inhalt

Problem

Bei der Implementierung von Cisco Secure Access VPN treten auf Jabber-Clients aufgrund von Konflikten bei der Auflösung von DNS-SRV-Datensätzen Verbindungsprobleme auf. Das Problem tritt auf, wenn Jabber zwei DNS SRV-Einträge erreicht: eine für den CUCM (_cisco-UDS) und eine für ExpressWay (_collab-edge). Wenn der CUCM SRV-Datensatz aufgelöst wird, geht Jabber unabhängig davon, ob er funktioniert, davon aus, dass er vor Ort ist, und versucht, eine Verbindung zum CUCM statt zu ExpressWay herzustellen. Dieses Verhalten zeigt sich in der Jabber-Protokollierung mit dem bEdgeServerFlag = 0, wie in Jabber.log zu sehen ist. Außerdem schlägt der ExpressWay SRV-Eintrag fehl, da er an den privaten DNS-Server gesendet wird, den der Secure Client für die Auflösung verwendet, und der private DNS-Server diesen öffentlichen SRV-Eintrag nicht rekursiv findet.

Umwelt

- Cisco Secure Access (ehemals Cisco AnyConnect Secure Mobility Client)
- Cisco Jabber-Client
- Cisco Unified Communications Manager (CUCM)
- Cisco ExpressWay für Mobil- und Remote-Zugriff
- DNS-Infrastruktur mit privaten und öffentlichen DNS-Servern
- VPN-Tunnelkonfiguration mit Split-Tunneling-Funktionen

Auflösung

Das Problem wurde behoben, indem Jabber-Datenverkehr durch den VPN-Tunnel geleitet wurde, anstatt zu versuchen, den Client manuell für die ExpressWay-Verbindung zu konfigurieren. Mit diesem Ansatz wird sichergestellt, dass der Jabber-Datenverkehr den geeigneten DNS-Auflösungspfad verwendet und ein SRV-Datensatzkonflikt vermieden wird, der dazu führt, dass der Client die Verbindung vor Ort fälschlicherweise übernimmt.

Schritte zur Fehlerbehebung

Schritt 1: Analysieren Sie DNS SRV-Eintragsabfragen mithilfe von Wireshark Packet Capture.

Use Wireshark filter: `dns.qry.type == 33`

Phase 2: Überprüfung der Jabber-Protokolle auf den Flagstatus des Edge-Servers

Check Jabber.log for: `bEdgeServerFlag = 0`

Schritt 3: Überprüfung des DNS-Auflösungsverhaltens für beide SRV-Datensätze

Prüfauflösung von:

- `_cisco-UDS` SRV-Datensatz (CUCM)
- `_Collaboration-Edge` SRV-Datensatz (ExpressWay)

Implementierung der Lösung

Konfigurieren Sie den Cisco Secure Access VPN-Client so, dass er Jabber-Datenverkehr in den Tunnel einbindet, anstatt DNS-Abfragen über den lokalen/privaten DNS-Server auflösen zu können. Dadurch wird sichergestellt, dass

- Jabber-Datenverkehr verwendet den richtigen DNS-Auflösungspfad
- SRV-Datensatzkonflikte werden vermieden

- Die ExpressWay-Verbindung ist ordnungsgemäß eingerichtet.
- Vollständige Jabber-Funktionalität bleibt erhalten

Diese Lösung wird gegenüber der manuellen Konfiguration des Jabber-Clients für ExpressWay bevorzugt, was den Verlust bestimmter Funktionen zur Folge hätte.

Ursache

Die Ursache liegt in der Auflösungslogik der DNS SRV-Einträge auf Jabber-Clients. Beim Start fragt Jabber nach zwei spezifischen DNS SRV-Datensätzen ab: `_cisco-UDS` (für CUCM) und `_collab-edge` (für ExpressWay). Bei der Entscheidungsfindung des Clients wird der CUCM SRV-Datensatz priorisiert. Wenn dieser Datensatz erfolgreich aufgelöst wird, geht Jabber davon aus, dass er in einer lokalen Umgebung ausgeführt wird, und setzt `bEdgeServerFlag = 0`, unabhängig davon, ob die tatsächliche CUCM-Verbindung funktioniert oder ob der ExpressWay SRV-Datensatz ebenfalls aufgelöst wird.

In VPN-Szenarien mit Split-Tunneling wird der ExpressWay SRV-Datensatz (`_collab-edge`) an den privaten DNS-Server gesendet, der vom Secure Client verwendet wird. Da es sich hierbei in der Regel um einen öffentlichen DNS-Eintrag handelt und der private DNS-Server keine rekursiven Suchvorgänge nach externen Datensätzen durchführt, schlägt die Auflösung der ExpressWay SRV fehl. Aufgrund dieses komplexen Problems ist Jabber nicht in der Lage, über beide Pfade die richtige Verbindung herzustellen.

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.