Secure Access VPN - kein Zugriff auf Jabber

Inhalt

Problem

Secure Client-Benutzer konnten nicht über den Secure Access VPN-Tunnel auf interne und private Anwendungen wie Jabber und Epic zugreifen, wenn sie eine private Zugriffsrichtlinie verwendeten. Bei dem Versuch, diese wichtigen Geschäftsanwendungen über die VPN-Verbindung zu erreichen, traten bei den Benutzern Verbindungsfehler auf. Während der Fehlerbehebung wurde unidirektionaler Datenverkehr für Epic-Ressourcen beobachtet, bei denen Ping- und TCP-SYN-Datenverkehr den VPN-Tunnel für sicheren Zugriff verlor. Bei der Palo Alto-Firewall wurden jedoch Probleme bei der Validierung des zurückkehrenden Datenverkehrs festgestellt. Darüber hinaus wurden Probleme mit der Jabber-Erreichbarkeit dokumentiert, bei denen CUCM-FQDNs über interne DNS auflösten, während die Datenverkehrssteuerung für IP-basiertes Routing konfiguriert war, was zu einer Diskrepanz im Datenverkehrsfluss führte.

Umwelt

- Cisco Secure Access mit VPN-Tunnelkonfiguration
- Sicherer Client für VPN-Verbindungen
- Implementierung von Richtlinien für privaten Zugriff
- Cisco Unified Communications Manager (CUCM) für Jabber-Services
- Epische Anwendungsressourcen
- Palo Alto Firewall für Netzwerksicherheit
- Interne DNS-Auflösung für CUCM-FQDNs

Auflösung

Die Lösung umfasste mehrere Konfigurationsänderungen und Schritte zur Fehlerbehebung, um die Verbindung zu internen Anwendungen über den Secure Access VPN-Tunnel wiederherzustellen:

Subnetzkonfiguration und Tunneländerungen

Schritt 1: Hinzufügen zusätzlicher Subnetze zum VPN-Tunnel

Der VPN-Tunnelkonfiguration für die betroffenen Ressourcen wurden weitere Subnetze hinzugefügt. Nach der Implementierung dieser Änderung wurden die Ressourcen, auf die zuvor nicht zugegriffen werden konnte, erfolgreich geladen.

Konfiguration der CUCM-IP-Adresssteuerung

Phase 2: Konfigurieren der CUCM-IP-Steuerung

Zur Behebung des Jabber-Verbindungsproblems, bei dem die CUCM-FQDNs über interne DNS-Verbindungen während der IP-basierten Verkehrssteuerung auflösten, wurden die CUCM-IP-Adressen in den Secure Client geleitet. Durch diese Konfigurationsänderung wurde die DNS-Auflösung an den Verkehrssteuerungsmechanismus angepasst.

Schritt 3: Zugriffsrichtlinien-Regel erstellen

Es wurde eine Zugriffsrichtlinienregel erstellt, um den Zugriff auf die CUCM-IP-Adressen zu ermöglichen. Durch diese Regel wurde die ordnungsgemäße Verbindung zur CUCM-Infrastruktur wiederhergestellt, und die Jabber-Funktion über den VPN-Tunnel wurde aktiviert.

Konfigurieren von statischem Routing

Schritt 4: Konfigurieren von statischem Routing für das CUCM-Subnetz

Stellen Sie sicher, dass die CUCM-IP-Adressen und das gesamte CUCM-Subnetz in der statischen Routing-Tabelle für den Netzwerktunnel enthalten sind. Durch diese Konfiguration wird das ordnungsgemäße Routing des Datenverkehrs zwischen dem Secure Client-Benutzerpool und der CUCM-Infrastruktur sichergestellt.

Validierung des Rückverkehrs

Schritt 5: Validierung von Paketfluss und -rückverkehr

Validieren Sie die Konfiguration des Paketflusses, um sicherzustellen, dass der zurückkehrende Datenverkehr den Secure Client-Benutzerpool erreichen kann. Dazu gehört die Überprüfung der

Palo Alto Firewall-Konfiguration, um eine ordnungsgemäße Rückpfad-Validierung für alle internen Ressourcen sicherzustellen, insbesondere für Epic-Verbindungen, bei denen unidirektionaler Datenverkehr beobachtet wurde.

Ursache

Die Verbindungsprobleme wurden durch mehrere Konfigurationslücken in der Secure Access VPN-Implementierung verursacht:

- Fehlende Subnetzkonfigurationen im VPN-Tunnel verhinderten eine ordnungsgemäße Weiterleitung an interne Anwendungsressourcen.
- Diskrepanz zwischen DNS-Auflösung (FQDN-basiert) und Datenverkehrssteuerungskonfiguration (IP-basiert) für CUCM-Services verursachte Jabber-Verbindungsausfälle
- Unvollständige Zugriffsrichtlinien, die keinen Datenverkehr an CUCM-IP-Adressen zulassen
- Fehlende statische Routing-Einträge für CUCM-Subnetze in der Netzwerk-Tunnel-Konfiguration
- Probleme bei der Validierung von Rückverkehrspfaden an der Palo Alto-Firewall, die die bidirektionale Kommunikation beeinträchtigen

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.