Interner Serverfehler der Tunnelgruppe für sicheren Zugriff, primäre Peer-IP-Adresse zurückgesetzt

Inhalt

Problem

Beim Versuch, die Remote-Peer-IP in einer Network Tunnel Group (NTG) in Cisco Secure Access zu ändern, können Benutzer auf einen "Internal Server Error" in der Benutzeroberfläche stoßen, wenn sie versuchen, die primäre Tunnel-IP auf einen zuvor konfigurierten Wert zurückzusetzen. Das spezifische Szenario umfasst Folgendes:

- Ein NTG wurde anfänglich mit einer primären Tunnel-IP und einer sekundären IP-Adresse konfiguriert, wobei beide Tunnel erfolgreich eingerichtet wurden.
- Die primäre Tunnel-IP-Adresse wird zu Testzwecken in eine andere IP-Adresse geändert, was problemlos akzeptiert wird.
- Wenn versucht wird, die primäre Tunnel-IP auf den ursprünglichen Wert zurückzusetzen, kann das System die Konfiguration nicht speichern und gibt einen "Internal Server Error" (Interner Serverfehler) in der Benutzeroberfläche zurück.
- Dieses Verhalten ist konsistent reproduzierbar und tritt auf, wenn versucht wird, eine zuvor konfigurierte IP-Adresse wiederzuverwenden.
- Die ursprüngliche IP-Adresse funktionierte bereits, und es gibt keine Konflikte mit der sekundären Tunnel-IP-Adresse.

Umwelt

- Cisco Secure Access (ehemals Cisco Umbrella für SSE)
- Konfiguration der Netzwerk-Tunnelgruppe für privaten Zugriff

- Dual-Tunnel-Konfiguration mit primären und sekundären Peer-IPs
- Webbasierte Management-Oberfläche

Auflösung

Dieses Problem wird durch ein Backend-Validierungs-/Statusproblem verursacht, bei dem die ursprüngliche Peer-IP nach Konfigurationsänderungen reserviert bleibt oder im Backend-System verbleibt. Befolgen Sie die Schritte zur Fehlerbehebung, die im nächsten Abschnitt beschrieben werden:

Schritt 1: Diagnoseinformationen erfassen

Sammeln Sie die folgenden Informationen für die Backend-Validierung:

- Organisations-ID für sicheren Zugriff
- Name der Netzwerk-Tunnelgruppe
- Tunnel-ID für den betroffenen primären Tunnel
- Für NTG ausgewählte Region/Rechenzentrum
- Exakter Zeitstempel eines fehlgeschlagenen Speicherversuchs, einschließlich Zeitzone
- Bestätigung, ob die ursprüngliche IP-Adresse in einem anderen NTG, aktuellen oder vorherigen angezeigt wird
- Browser-HAR-Erfassung des fehlgeschlagenen Speicherversuchs

Phase 2: HAR-Datei des Erfassungsbrowsers

So sammeln Sie Diagnosedaten für den fehlgeschlagenen Speicherversuch:

- Browser öffnen Entwickler-Tools
- Registerkarte "Netzwerk" aufrufen

- Protokoll beibehalten aktivieren
- Reproduzieren des Speicherfehlers
- Exportieren Sie die HAR-Datei, und hängen Sie sie an den Supportfall an.

Anmerkung: Vor dem Hochladen der HAR-Datei sollten Session-Token oder Cookies gesäubert bzw. entfernt werden.

Schritt 3: Backend-Validierung und -Bereinigung

Dieses Problem erfordert Backend-Eingriffe und kann nicht allein über die Benutzeroberfläche gelöst werden. Der technische Support von Cisco muss die folgenden Aktionen durchführen:

- Sicherer Zugriff durch Backend-/SSE-Plattform-Team
- Für veraltete Peer-IP-Reservierung validieren
- Suche nach verwaisten Tunnelobjekten
- Identifizieren Sie doppelte Backend-Schlüssel, die mit der jeweiligen NTG-Konfiguration verknüpft sind.
- Löschen Sie den veralteten Tunnelpeer-Verweis für die ursprüngliche IP.
- Erzwungene Backend-Re-Synchronisierung von NTG-Objekten (falls erforderlich)
- Freigabe der Peer-IP-Zuweisung an die NTG UUID

Schritt 4: Alternative Auflösungsmethode

Wenn die Backend-Bereinigung nicht sofort verfügbar ist, gehen Sie folgendermaßen vor:

- Löschen der primären Konfiguration der Netzwerk-Tunnelgruppe
- 5 Minuten warten
- NTG mit der erforderlichen IP-Adresse erneut hinzufügen

⚠Vorsicht: Möglich. Die hier genannten Details enthalten offenbar Prozeduren oder Befehle, die bei ihrer Ausführung erhebliche Auswirkungen haben könnten. Stellen Sie sicher, dass die oben genannten Verfahren oder Befehle von einem SME oder einem Geschäftsbereich evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Schritt 5: Temporäre Problemumgehung

Wenn das NTG in Produktion ist und nicht entfernt werden kann:

- Den sekundären Tunnel weiterhin für die Konnektivität verwenden
- Holen Sie sich eine alternative öffentliche IP von Ihrem Anbieter/Partner
- NTG-Primärverbindung aktualisieren, um die alternative IP zu verwenden
- Bestätigen Sie eine reduzierte Redundanz, bis das Backend-Problem behoben ist.

Ursache

Dieses Problem wird durch einen Softwarefehler im Cisco Secure Access-Backend-System verursacht. Wenn eine primäre Peer-IP geändert und auf ihren ursprünglichen Wert zurückgesetzt wird, behandelt das Backend-Validierungssystem die ursprüngliche IP fälschlicherweise als noch zugewiesen oder reserviert, selbst wenn sie für die Wiederverwendung verfügbar sein sollte. Dies führt zu einem Backend-Validierungsfehler, der von der Benutzeroberfläche als generischer "interner Serverfehler" maskiert wird. Das Backend-System kann die IP-Reservierung während des Konfigurationsänderungsprozesses nicht ordnungsgemäß bereinigen oder freigeben, wodurch ein dauerhaftes Zustandsproblem entsteht, das verhindert, dass die IP im selben NTG wiederverwendet wird.

Verwandte Inhalte

- Fehlerbehebung und Erfassung grundlegender Informationen für Cisco Secure Access
- 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.