

Problem mit der IPsec-Tunnelverbindung für sicheren Zugriff beim Versa Networks-Router aufgrund von ESN-Verhandlungen

Inhalt

Problem

Bei der Bereitstellung von Cisco Secure Access in einer Zweigstelle mit Versa-Network Router als Edge-Gerät traten Verbindungsprobleme auf, obwohl beide IPsec-Tunnel betriebsbereit erschienen. T

Zu den spezifischen Symptomen gehören:

- Keine Verbindung von der Zweigstelle zu Cisco Secure Access
- Internetzugang über statische Routen nicht funktionsfähig
- Beobachteter unidirektionaler verschlüsselter Datenverkehr (nur ausgehend zu sicherem Zugriff)
- Routerstatistiken mit gesendeten, aber nicht empfangenen ausgehenden Paketen
- Dead Peer-Erkennung funktioniert bidirektional zwischen SD-WAN-Router und sicherem Zugriff
- Security Parameter Index (SPI)-Werte für ausgehenden Datenverkehr stimmen korrekt überein
- Das Verbindungsproblem konnte durch das Tunnel-Flapping (Zurücksetzen) nicht behoben werden.
- Paketerfassungen und Screenshots bestätigen den Mangel an eingehendem Datenverkehr.
- Das Problem konnte durch Ändern der Tunnelchiffre von CBC in GCM nicht behoben werden.

Die Untersuchung ergab, dass der Datenverkehr auf Cisco Seite aufgrund von Prüfsummenfehlern nicht entschlüsselt werden konnte. Diese Fehler wurden auf den Versa-

Router zurückgeführt, der die ESN-Funktion (Extended Sequence Number) aushandelte.

Umwelt

- Cisco Secure Access-Bereitstellung
- Versa-Networks-Router als Edge-Gerät
- Konfiguration des IP-Identitätstunnels
- IPsec-Tunnelkonfiguration mit CBC- und GCM-Verschlüsselungsversuchen

Auflösung

Die Auflösung beinhaltete das Deaktivieren der Extended Sequence Number (ESN)-Aushandlung auf dem Versa-Router, um Prüfsummenfehler zu vermeiden, die Entschlüsselungsfehler auf dem Cisco Secure Access-Headend verursacht haben.

Schritte zur Problembehebung

Schritt 1: Identifizieren der Ursache

Die Untersuchung ergab, dass der Versa-Router eine erweiterte Sequenznummer (ESN) aushandelte, was dazu führte, dass das Headend von Cisco Secure Access Prüfsummenfehler empfing und die von ESN erstellten Pakete nicht entschlüsselte.

Phase 2: ESN auf dem Versa-Router deaktivieren

Wenden Sie sich an den Versa Networks-Support oder an den Router-Administrator, um ESN-Prüfungen und Verhandlungen für die Versa Router-Konfiguration zu deaktivieren. Damit wird der

bekannte Versa-Fehler behoben, der dazu führt, dass ESN nicht ordnungsgemäß ausgehandelt wird.

Schritt 3: Konnektivität überprüfen

Stellen Sie nach der Deaktivierung der ESN-Aushandlung sicher, dass der bidirektionale Datenverkehrsfluss hergestellt und die vollständige Verbindung von der Außenstelle zu Secure Access und zum Internet wiederhergestellt ist.

Schritt 4: Datenverkehrsflussüberwachen

Überprüfen Sie, ob die Statistiken für ein- und ausgehende Pakete auf dem Router den richtigen Datenverkehrsfluss in beide Richtungen anzeigen, und bestätigen Sie so, dass das Problem des unidirektionalen Datenverkehrs erfolgreich behoben wurde.

Ursache

Die Ursache wurde als bekannter Versa-Netzwerk-Fehler identifiziert (Versa-Support-Bug-ID: 122437 - ESN darf nicht von VOS ausgehandelt werden, wenn der Versa-Router während der Einrichtung des IPsec-Tunnels die ESN-Funktion (Extended Sequence Number) falsch aushandelt. Diese ESN-Aushandlung bewirkt, dass das Headend von Cisco Secure Access Pakete mit Prüfsummenfehlern empfängt, die korrekte Entschlüsselung verhindert und einen unidirektionalen Datenverkehrsfluss zur Folge hat. Der Versa-Router sendet ausgehende Pakete erfolgreich, aber der zurückgehende Datenverkehr kann aufgrund von ESN-bezogenen Entschlüsselungsfehlern nicht ordnungsgemäß verarbeitet werden.

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.