Übermäßige DNS-Anforderungen an Port 53 während AnyConnect VPN-Sitzungen

Inhalt

Problem

Nach der Implementierung von Remote Access VPN (RA-VPN) generieren Benutzer, die sich über Cisco AnyConnect verbinden, Dutzende von DNS-Anfragen an Port 53 an den sekundären DNS-Server. Dieses Verhalten wird in der Aktivitätsüberwachung für alle Benutzer beobachtet, die mit dem VPN-Tunnel verbunden sind, und führt dazu, dass zahlreiche zulässige Anforderungen den Tunnel überfluten. Diese übermäßige DNS-Aktivität tritt nicht auf, wenn Benutzer eine Verbindung über ZTA (Zero Trust Access) herstellen. Dies weist darauf hin, dass das Problem speziell mit der AnyConnect VPN-Verbindungsmethode zusammenhängt.

Umwelt

- Produktfamilie: Sicherer Zugriff
- Implementierung: Remote Access-VPN-Bereitstellung
- Vergleichsumgebung: ZTA (Zero Trust Access) - Nicht das gleiche DNS-Flooding-Verhalten

Auflösung

Die Untersuchung übermäßiger DNS-Anfragen erfordert eine Protokollsammlung und -analyse, um die Ursache des DNS-Flooding-Verhaltens zu ermitteln. Die Protokollerfassung umfasst das Erfassen der Paketerfassung mit der PID für jedes Paket, um zu bestimmen, welche Anwendung auf einem Endpunkt den Datenverkehr und die Prozessmonitorausgabe generiert.

Ursache

Die Analyse hat ergeben, dass diese Menge an DNS-Datenverkehr erwartet wird.

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.