Fehlerbehebung der Kompatibilität zwischen Netskope und dem Umbrella Roaming Client

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Kompatibilitätsprobleme zwischen Netskope und dem Umbrella-Roaming-Client behoben werden.

Überblick

Diese KBA richtet sich an Benutzer des Netskope-Proxys, bei denen ein Problem auftritt, bei dem der Roaming-Client nicht mit dem Umbrella Dashboard synchronisiert werden kann. Dies führt dazu, dass der Roaming-Client im Netzwerk nicht ordnungsgemäß aktiviert wird. In diesem Artikel wird das Ausschließen unserer Synchronisierungen aus dem Netskope-Proxydienst erläutert.

Diese Informationen gelten für Roaming-Clients unter Windows und MacOS.

Auswirkungen

Wenn SSL über den Netskope-Proxy getunnelt wird und SSL-Datenverkehr an Netskope-Server weiterleitet, kann der Roaming-Client nicht erfolgreich mit Umbrella synchronisiert werden. Dies führt dazu, dass sie in einem ungeschützten, unverschlüsselten Zustand verbleibt. In einigen Fällen kann der Client vor der ersten Synchronisierung verschlüsselt werden. Dies führt zu einem bekannten Problem, das dazu führt, dass interne Domänen (die nicht in der lokalen DNS-Suffixliste enthalten sind) nicht aufgelöst werden können.

Mehrere native Apps verhalten sich mit Netskope so, als wären sie mit einem Zertifikat verbunden, was dazu führt, dass Zertifikate von Drittanbietern nicht akzeptiert werden. Diese Pin-Belegung erfolgt aufgrund des .NET-Krypto-Frameworks, das vom Roaming-Client verwendet wird.

Auflösung: Roaming-Client vom Proxy umgehen

Die Lösung besteht darin, den Serviceprozess des Roaming-Clients von der Weiterleitung über den Netskope-Proxy über dessen "Certificate Pinned Applications"-Funktion auszuschließen.

Wenn Anwendungen definiert sind, können sie eine App blockieren oder umgehen. Wenn Sie

Bypass (für die Roaming-Client-Synchronisierung erforderlich) auswählen, leitet der Netskope-Client keinen Datenverkehr vom Endpunkt zum Netskope-Proxy in der Cloud, und die Apps funktionieren weiterhin. Wenn Sie Blockieren auswählen, wird der Datenverkehr vom Netskope-Client blockiert. Standardmäßig werden alle Apps umgangen. Die erforderliche Einstellung ist jedoch, den Dienst des Roaming-Clients zu umgehen.

Gehen Sie folgendermaßen vor, um mit Zertifikaten verbundene Anwendungen zu bearbeiten und den Umbrella-Roaming-Client-Dienst hinzuzufügen:

1. Navigieren Sie zu Einstellungen > Verwalten > Zertifikatfixierte Anwendungen > Erweiterte Einstellungen. Das Fenster Erweiterte Einstellungen wird angezeigt.
2. Wählen Sie im Fenster Erweiterte Einstellungen die Option Benutzerdefinierte Einstellungen für jede Anwendung aus. Gehen Sie wie folgt vor, um einen benutzerdefinierten Service/eine benutzerdefinierte Anwendung hinzuzufügen.
    - Wählen Sie in der Liste Anwendung die Option Microsoft Office 365 Outlook.com aus (es gibt keine Umbrella-Option, die es uns ermöglicht, fortzufahren), und wählen Sie unter Aktion die Option Umgehen aus.
    - Wählen Sie als Modus Direkt aus.
    - Geben Sie im Feld "Plugin Process" (Plugin-Prozess) "ercservice.exe" für den eigenständigen Roaming-Client ein. Geben Sie für das AnyConnect-Roaming-Modul "acumbrellaplugin.exe" ein.
3. Klicken Sie auf Senden. Die erweiterten Einstellungen werden geschlossen.
4. Starten Sie auf dem Client-Computer den Netskope-Agenten neu, um diese neuen Einstellungen sofort zu übernehmen. (Normalerweise wird der Client innerhalb einer Stunde aktualisiert, wenn die Clients sich an Netskope wenden.)

Erweiterte Einstellungen sind vorhanden. Es wird angenommen, dass eines der beiden Szenarien funktioniert. Bypass + direct wird jedoch empfohlen.

1. Umgehung + Direkt: Bei Auswahl dieser Option werden die konfigurierten Apps/Domänen vom Client umgangen. Es reist nicht nach Netskope.
2. Umgehung + Tunnel: Bei Auswahl dieser Option tunnelt der Client den Datenverkehr von Anwendungen/Domänen, wird jedoch vom Netskope-Proxy umgangen. Diese Option ist für Domänen nützlich, die einem SSO-Authentifizierungsdienst zugeordnet sind, da diese Dienste die Quell-IP der Netskope-Cloud verwenden, um zu ermitteln, ob der Zugriff auf die Cloud-App durch Netskope geschützt ist.

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.