Probleme mit dem MacOS-Internetzugriff nach dem Importieren des Zertifikats für sicheren Zugriff

Inhalt

Problem

MacOS-Benutzer können nach dem Importieren des Internetzertifikats aus dem Portal nicht mehr über Cisco Secure Access auf Internetressourcen zugreifen.

Betroffene Services:

- Microsoft Outlook (Senden und Empfangen)
- Google.com
- AI-Websites
- Andere Webziele

Windows-Benutzer mit derselben Konfiguration sind davon nicht betroffen und funktionieren weiterhin normal. Das Problem betrifft speziell den Zugriff von MacOS-Clients auf E-Mails und allgemeine Internetbrowsing-Funktionen nach dem Zertifikatimport.

Umwelt

- Cisco Secure Access mit Unified Policy-Konfiguration
- MacOS-Clients mit importiertem Internetzertifikat aus dem Cisco Secure Access-Portal
- Windows-Clients mit gleicher Konfiguration (nicht betroffen)
- Verwendete Internetrichtlinien, private Richtlinien, SvD-Richtlinien, RBI und

Sicherheitsprofile

- Gemischte Betriebssystemumgebung mit unterschiedlichem Verhalten zwischen MacOS und Windows

Auflösung

Die Lösung beinhaltet das Hinzufügen spezifischer Microsoft Outlook-Endpunkte und -Anwendungen zur DND-Liste (Do Not Decrypt), um die SSL-Überprüfung für diese Dienste zu umgehen.

Schritt 1: Hinzufügen von Outlook-Endpunkten zur DND-Liste

Fügen Sie die in den nächsten Abschnitten beschriebenen Endgeräte oder Anwendungen zur Konfiguration Nicht entschlüsseln (DND) hinzu, um die Zugriffsprobleme mit Outlook zu beheben.

```
outlook.cloud.microsoft
outlook.office.com
outlook.office365.com
smtp.office365.com
```

Phase 2: Auflösung überprüfen

Nachdem Sie die Outlook-bezogenen Endpunkte zur DND-Liste hinzugefügt haben, stellen Sie sicher, dass die betroffenen MacOS-Clients jetzt auf Folgendes zugreifen können:

- Microsoft Outlook-Funktion zum Senden und Empfangen
- Andere zuvor betroffene Internetressourcen

Der Benutzer bestätigte, dass nach der Implementierung dieser DND-Einträge die Outlook-Anwendungen weiterhin normal auf MacOS-Geräten funktionieren.

Ursache

Das Problem wurde durch eine SSL/TLS-Verschlüsselungsprüfung verursacht, die die Fähigkeit der MacOS-Clients beeinträchtigte, sichere Verbindungen zu Internetressourcen, insbesondere zu Microsoft Outlook-Diensten, herzustellen. Der Prozess der Verschlüsselungsprüfung verhinderte eine ordnungsgemäße Zertifikatsvalidierung oder den Verbindungsaufbau speziell auf MacOS-Plattformen, während Windows-Clients nicht von den gleichen Überprüfungsrichtlinien betroffen waren. Durch Hinzufügen der betroffenen Endpunkte zur Liste "Nicht entschlüsseln" wird die Überprüfung für diese spezifischen Dienste umgangen, sodass die normale Verbindung wieder hergestellt werden kann.

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.