Umbrella-Proxy blockiert Ninja-Anwendungsverbindungen

Inhalt

Problem

Benutzer können ein Remote-System nicht mit einer heruntergeladenen Setup-Datei ausführen, wenn eine Verbindung über Cisco Umbrella besteht. Die Anwendung funktioniert nicht unter Umbrella Protection, was sich speziell auf den Zugriff auf das Remote-System auswirkt. Das gleiche Remote-System funktioniert einwandfrei und problemlos, wenn der Cisco Umbrella Proxy deaktiviert ist.

Zu den Versuchen der Fehlerbehebung zählten Tests mit einer separaten Richtlinie, bei der die Systemsicherheit und das Ziel auf ANY festgelegt wurden, das Problem jedoch weiterhin bestand. Zusätzlich wurde versucht, den Datenverkehr über Zero Trust Access (ZTA) zu leiten, das Problem blieb jedoch unverändert. Der Datenverkehr wurde über Secure Access über TCP/443 zugelassen, die Verbindungen wurden jedoch auf dem Endgerät weiterhin blockiert.

Umwelt

- Cisco Umbrella mit aktivierter Proxy-Funktion
- ZTA-Konfiguration (Zero Trust Access)
- Für TCP/443-Datenverkehr konfigurierte Richtlinien für sicheren Zugriff

Auflösung

Die Lösung beinhaltet das Ausschließen bestimmter NinjaOne-bezogener Domänen vom Umbrella-Proxy, um eine direkte Konnektivität für die Remote-Zugriffsanwendung zu ermöglichen.

Schritt 1: Betroffene Domänen identifizieren

Die Analyse der Paketerfassung und der HAR-Dateien zeigt, dass diese NinjaOne-bezogenen Domänen vom Umbrella-Proxy betroffen sind:

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Phase 2: Domänenausnahmen konfigurieren

Schließen Sie die identifizierten Domänen sowohl von den Richtlinien für die Internetsicherheit des Secure Web Gateway (SWG) als auch von der Steuerung des ZTA-Internetdatenverkehrs aus. Diese Konfigurationsänderung ermöglicht es diesen Domänen, den Umbrella-Proxy zu umgehen und direkte Verbindungen herzustellen.


Anmerkung: Eine DND-Listenkonfiguration (Do Not Decrypt) hat sich zur Behebung dieses Problems als unwirksam erwiesen. Die Verkehrssteuerung und -befreiung wird empfohlen.

Schritt 3: Konfigurationsänderungen anwenden

Implementieren Sie die Domänenausnahmen in der Umbrella-Konfiguration, um den NinjaOne-bezogenen Datenverkehr von der Proxy-Verarbeitung auszuschließen. Dadurch kann die Remote-Zugriffsanwendung direkte Verbindungen zu den erforderlichen Services herstellen.

Schritt 4: Auflösung überprüfen

Testen Sie die Anwendungsfunktionalität für den Remote-Zugriff nach der Anwendung der Ausnahmen, um sicherzustellen, dass die richtige Verbindung wiederhergestellt wird, während Umbrella-Schutz für anderen Datenverkehr beibehalten wird.

Ursache

Das Problem tritt auf, weil NinjaOne-Anwendungen für den Remote-Zugriff Proxyverbindungen ablehnen, wenn der Datenverkehr über den Cisco Umbrella-Proxy geleitet wird. Die Anwendung erfordert eine direkte Verbindung zu bestimmten NinjaOne-Domänen, um ordnungsgemäß zu funktionieren. Wenn diese Verbindungen über Umbrella als Proxy bereitgestellt werden, kann der Remote-Zugriffsdienst nicht die erforderlichen Kommunikationskanäle einrichten, was zu einem Anwendungsfehler führt, selbst wenn Sicherheitsrichtlinien konfiguriert sind, die den Datenverkehr zulassen.

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.