

Umbrella代理阻止Ninja應用程式連線

目錄

問題

通過Cisco Umbrella連線時，使用者無法使用下載的安裝程式檔案運行遠端系統。應用程式在Umbrella保護下無法正常工作，具體影響對遠端系統的訪問。禁用Cisco Umbrella代理時，同一個遠端系統可以正常工作而不會出現任何問題。

故障排除嘗試包括使用單獨的策略進行測試，在該策略中系統安全和目標設定為ANY，但問題仍然存在。此外，已嘗試透過零信任存取(ZTA)路由流量，但問題保持不變。流量允許通過TCP/443上的安全訪問，但連線仍被終端阻止。

環境

- 已啟用代理功能的思科資安防護傘
- 零信任訪問(ZTA)配置
- 為TCP/443流量配置的安全訪問策略

解析

解決方案涉及從Umbrella代理中排除特定的NinjaOne相關域，以允許遠端訪問應用程式的直接連線。

步驟 1: 確定受影響的域

對資料包捕獲和HAR檔案的分析表明，這些與NinjaOne相關的域受Umbrella代理的影響：

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

步驟 2:配置域免除

從安全Web網關(SWG)Internet安全策略和ZTA網際網路流量引導中排除標識的域。此配置更改允許這些域繞過Umbrella代理並建立直接連線。



附註：發現不解密(DND)清單配置對於解決此問題無效。流量引導和免除是推薦的方法。

步驟 3:應用配置更改

在Umbrella配置中實施域免除，以從代理處理中排除與NinjaOne相關的流量。這樣，遠端訪問應用程式就可以建立到所需服務的直接連線。

步驟 4:驗證解決方案

在應用免除後測試遠端訪問應用程式功能，以確保恢復正確的連線，同時保持對其他流量的Umbrella保護。

原因

出現此問題的原因是，當流量通過Cisco Umbrella代理路由時，NinjaOne遠端訪問應用程式會拒絕代理連線。應用程式需要直接連線到特定的NinjaOne域才能正常工作。當通過Umbrella代理這些連線時，遠端訪問服務無法建立必要的通訊通道，導致應用程式故障，即使將安全策略配置為允許流量也是如此。

相關內容

- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。