防止使用者使用UltraSurf

目錄

簡介

本文檔介紹如何防止使用者使用UltraSurf。

問題

使用者使用UltraSurf代理繞過內容過濾和安全配置。

原因

UltraSurf結合了多種措施，可避免使用常用的內容過濾解決方案。它使用SSL建立到遠端主機的連線，以加密資料並防止大多數解決方案進行「窺探」。

目前，UltraSurf會進行更改以降低瀏覽器的安全設定，因為它使用無效的SSL證書來建立這些連線。在以前的版本中，UltraSurf使用DNS作為繞過內容過濾解決方案的機制，而Umbrella通過識別這些DNS伺服器並阻止訪問它們來降低其速度。不過，UltraSurf背後的團隊一直在不斷發佈新版軟體，因此他們再次改變做法只是時間問題。

解決方案

還可以採取其他措施，包括阻止UltraSurf已知使用的子網。這些通常是ISP分配的動態IP範圍，只有很少甚至沒有商業使用者的合法用途。此外，在Active Directory環境中，可以使用軟體限制策略限制應用。這可用於限制當前和早期版本的UltraSurf軟體在您的網路上運行。

發佈新版本後，您需要新增其他軟體限制策略。還可以限制使用者對Internet Explorer的安全選項所做的更改，以防止使用無效的安全證書。我們將繼續監控Ultrasurf在每個修訂版中進行的版本和更改，並瞭解Umbrella如何幫助防止Ultrasurf訪問。

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）。