

使用GPO在Firefox和Chrome中維護DoH

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[概觀](#)

[Firefox](#)

[鉻合金](#)

簡介

本文說明如何使用Cisco Umbrella中的組策略對象(GPO)在Firefox和Chrome中維護和禁用HTTPS(DoH)上的DNS。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

透過HTTPS進行的DNS(DoH)是新增到多種Web瀏覽器的一項功能，允許DNS繞過透過HTTPS進行的系統DNS堆疊。在許多情況下，您可以禁用此功能以確保Web瀏覽器不會覆蓋任何Umbrella設定。

Firefox和Chrome都提供DoH功能，並且能夠阻止在您的網路和受管電腦上使用DoH。但是，DoH實現在瀏覽器之間有很大差異。

Firefox

Firefox使用預設的DoH設定運行，其中預設情況下將DNS傳送到CloudFlare 1.1.1。此設定不考慮系統DNS設定。

要對抗此問題，Umbrella預設將替代設定為禁用DoH（有關詳細資訊，請參閱本文中的文章）。但是，此覆蓋只有在沒有顯式設定的DoH設定時才會生效。要確保從未啟用DoH以將Firefox DNS從系統設定中轉移，需要GPO設定。

要禁用，請將「network.trr.mode」的值設定為0。有關詳細資訊，請參閱Firefox TRR設定。

有關在Firefox中管理企業策略的詳細資訊，請參閱Mozilla文檔。

鉻合金

Chrome為包括Umbrella在內的多家提供商提供對DoH的支援。與Firefox不同，Chrome DoH只有在系統DNS被視為參與的DNS提供商時才可啟用。因此，如果系統DNS是本地DNS伺服器或漫遊客戶端，則它無法啟用；但如果本地DNS是208.67.220.220和208.67.222.222，則它可啟用。因此，Chrome不會將您的DNS從系統DNS引出，而是使用DoH來增強它。

在Chrome DoH實驗的初始階段，如果裝置受管理、已加入AD或已應用企業策略，則Chrome可以禁用DoH。

有關詳細資訊，請參閱Chrome網站。

有關在Chrome中管理企業策略的更多資訊，請參閱Chrome文檔。

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）。