使用防火牆規則強制實施Umbrella DNS並防止繞過

目錄

簡介

本文說明如何使用防火牆規則和網路原則防止DNS繞過和執行Umbrella DNS保護。

必要條件

- 網路防火牆
- 防火牆訪問許可權
- 防火牆配置知識

實施Umbrella DNS — 最常見的方法

大多數路由器和防火牆允許您通過埠53強制實施所有DNS流量，要求所有網路裝置使用路由器上定義的DNS設定，該設定必須指向Umbrella DNS伺服器。

首選方法是將來自非Umbrella IP地址的所有DNS請求轉發到下面列出的Umbrella DNS IP。此方法透明地轉發DNS請求，並防止手動DNS配置簡單失敗。

或者，建立防火牆規則以僅允許DNS(TCP/UDP)到Umbrella DNS伺服器，並阻止所有其他DNS流量到任何其他IP地址。

防火牆規則示例

1. 將此規則新增到邊緣防火牆：
    - 允許TCP/UDP入站和出站到**208.67.222.222**或出**208.67.220.220**站埠53。
    - 阻止埠53上的所有IP地址的TCP/UDP入站和出站。

Umbrella DNS的允許規則優先於阻止規則。允許向Umbrella發出DNS請求，但阻止所有其他DNS請求。

根據您的防火牆配置介面，為每個協定配置單獨的規則，或為TCP和UDP配置一條規則。在網路邊緣裝置上應用規則。您還可以將類似的規則應用於工作站上的軟體防火牆，如Windows或macOS中的內建防火牆。

如果使用漫遊客戶端和Active Directory組策略，請參閱有關使用組策略鎖定企業漫遊客戶端的文檔。

透過HTTPS(DoH)強制執行DNS

建議的配置

1. 在Umbrella中，啟用Proxy / AnonymizerandDoH / DoTcontent類別。
2. 在防火牆上阻止已知DoH提供商的IP地址。

詳細資訊和背景

Umbrella支援use-application-dns.netMozilla定義的域，以防止Firefox在預設情況下啟用DoH。有關Firefox和DoH的資訊，請參閱相關文檔。

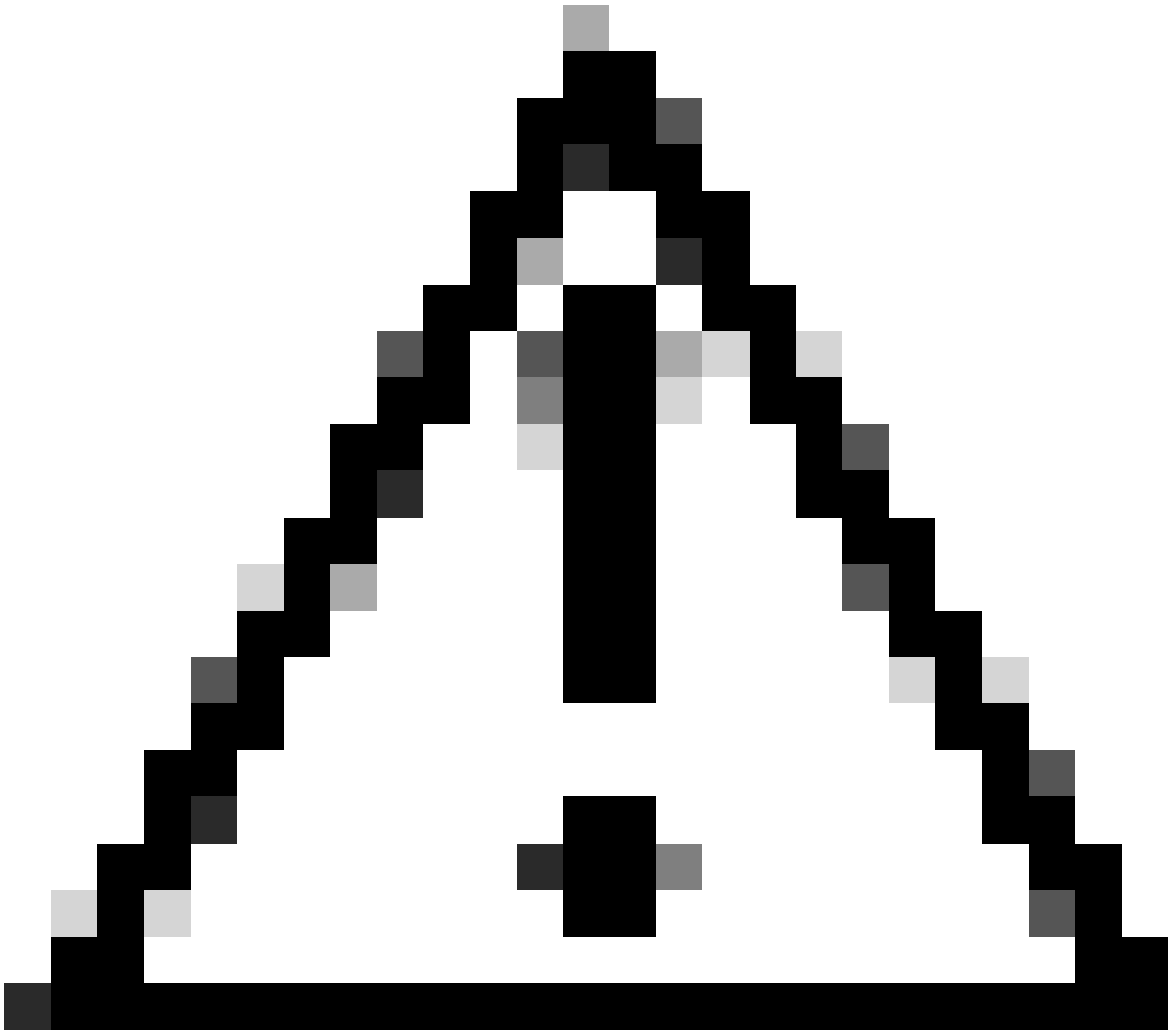
即使在阻止備用DNS提供程式之後，DNS仍然可以繞過DoH。本地DNS解析程式將DNS請求轉換為HTTPS，並使用JSON或POST/GET將其傳送到終結點。此流量通常可避免DNS檢查。

由於DoH可用於繞過Umbrella，因此Umbrella在Proxy/Anonymizer內容類別中包括已知的DoH伺服器。此機制有一些限制：

- 它無法阻止尚不瞭解的全新DoH提供商。
- 它不能阻止直接通過IP地址使用的DoH。

要處理新的DoH提供者，請監控更新並阻止新發現的域，以改善覆蓋範圍。

對於通過IP地址的DoH，場景是有限的。使用CloudFlare的Firefox就是一個突出的例子。



注意：請勿將Mozilla Kill Switch域新增到阻止清單中。阻止這些域將導致阻止頁面的A記錄，Firefox將此視為有效並自動升級其DoH使用情況。

通過TLS實施DNS(DoT)

即使在阻止備用DNS提供程式和DoH之後，也可以通過TLS繞過DNS，TLS在埠853上使用RFC7858。例如，CloudFlare是DoT提供程式。

實施示例

- 阻止IP地址1.1.1.1和1.0.0.1埠853(CloudFlare)。

防火牆支援簡介

本文檔幫助網路管理員實施Umbrella DNS。Cisco Umbrella支援不提供個別防火牆或路由器配置方面的幫助，因為每台裝置都有唯一的配置介面。請查閱路由器或防火牆文檔，或與裝置製造商聯絡，確認這些配置是否可行。

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）。