將Umbrella DNS與HTTP代理一起使用

目錄

簡介

本檔案介紹如何將Umbrella DNS與HTTP代理一起使用。

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Umbrella全域DNS服務，而不是為了安全網路閘道(SWG)。

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。

背景資訊

HTTP代理會攔截網路上的HTTP/S流量。然後，它代表原始客戶端與遠端伺服器建立HTTP/S連線，並將響應中繼回該客戶端。大多數HTTP代理有能力根據分類或安全內容阻止到特定站點的連線，或者阻止來自遠端伺服器的響應，這些響應會包含不需要的內容（如惡意軟體）。

將HTTP流量重新導向到Proxy有兩種主要方法：顯式重定向和透明重定向。這些不同的方法需要採取不同的步驟，才能與Umbrella結合正常發揮作用。

本文討論HTTP Proxy如何影響Umbrella的行為和Umbrella解決方案的每個部分，然後提供兩組明確重新導向和透明重新導向的步驟。

此圖是更詳細地概述的解決方案的摘要：

<table>
<tr><th></th><th>No Proxy</th><th>Transparent Proxy (Trusts Client DNS Resolution)</th><th>Transparent Proxy (Does Not Trust Client DNS Resolution)</th><th>Proxy Script</th><th>Explicit Proxy</th></tr>
<tr><td>Internet Connected
208.67.222.222 reachable over UDP 443</td><td colspan="2" rowspan="2">Umbrella protected</td><td colspan="3" rowspan="2">Web traffic via 80/443 resolved/protected by proxy

All other ports, Umbrella protected</td></tr>
<tr><td>Internet Connected
208.67.222.222 reachable over UDP 53</td></tr>
<tr><td>Internet Connected
No Umbrella access</td><td colspan="5" rowspan="2">Local DNS server used</td></tr>
<tr><td>No Internet access</td></tr>
</table>

proxy-umbrella-diagram.png

HTTP Proxy如何影響Umbrella全域DNS服務

當攔截HTTP/S流量時，HTTP代理會讀取HTTP/S請求中的主機標頭，並為該主機生成自己的DNS查詢。因此，在部署Umbrella解決方案時，必須考慮代理的行為。在抽象級別，這涉及確保到Umbrella IP地址的HTTP/S連線不會重定向到Proxy，而是直接傳送到其預期目標。

網路保護

當僅使用Umbrella網路保護時，建議將HTTP代理本身配置為直接使用Umbrella進行DNS解析，或者它可以使用內部DNS伺服器，後者進而將DNS查詢轉發到Umbrella。相應的外部IP地址可以在Umbrella Dashboard中註冊為網路標識。在這種情況下，無需執行其他操作即可使用Umbrella。

如果由於某種原因無法執行該操作，並且客戶端本身正在使用Umbrella，則可以採取本文中詳述的操作，以確保HTTP Proxy不會繞過實施。

Umbrella漫遊客戶端

使用Umbrella漫遊客戶端時，來自客戶端電腦的DNS查詢會直接傳送到Umbrella。但是，由於HTTP代理會執行自己的DNS查詢，因此Umbrella漫遊客戶端的強制會無效。因此，在代理環境中使用Umbrella漫遊客戶端時，必須遵守本文中詳述的操作。

虛擬裝置和Active Directory整合

虛擬裝置(VA)用作受保護網路上客戶端電腦的DNS伺服器。因此，使用HTTP Proxy會以與漫遊客戶端相同的方式使其執行無效。因此，可採取本條所詳述的行動，以確保執行有效且報告準確。

除了下面的操作之外，建議將HTTP Proxy配置為使用VA作為其DNS伺服器。這允許您定義特定於代理的策略，以便可以識別來自代理的查詢。這種策略還允許您禁用對源自代理的查詢的日誌記錄，從而避免在報告中出現重複的查詢。

顯性代理

部署顯式Proxy需要修改瀏覽器代理設定，以便將流量明確重定向到Proxy。這可以通過在Windows中使用組策略來實現，或者更常見的是通過使用代理自動配置(PAC)檔案來實現。無論哪種情況，都會使瀏覽器將所有HTTP流量直接傳送到代理，而不是傳送到遠端站點。因為瀏覽器知道Proxy會產生其自己的DNS請求，所以它不會費心解析遠端站點本身的主機名。此外，如前所述，當HTTP連線到達Proxy時，Proxy會生成它自己的DNS查詢，該查詢可得到與客戶端得到的結果不同的結果。

因此，為了與Umbrella一起正常工作，需要進行兩項更改：

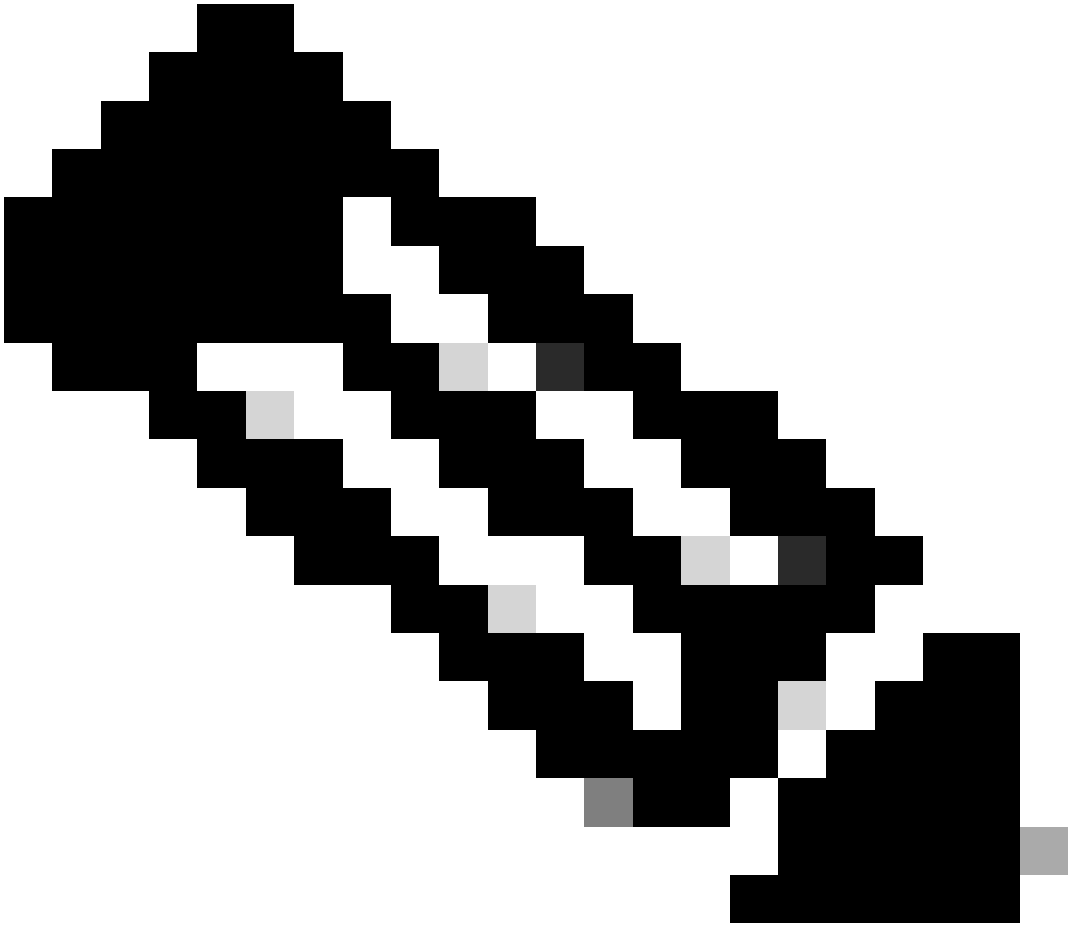
1. 必須強制客戶端進行DNS查詢。
2. 目的地為Umbrella IP位址的HTTP連線不得前往Proxy，而是直接前往Umbrella。

這兩種更改都可以使用PAC檔案完成：

```
function FindProxyForURL(url, host) {    // Generate DNS request on the client    hostIP = dnsResolve(h
        isInNet(hostIP, "155.190.0.0", "255.255.0.0") ||
        isInNet(hostIP, "146.112.0.0", "255.255.0.0")) ||
        isInNet(hostIP, "151.186.0.0", "255.255.0.0"))
    {         return "DIRECT";     }     // DEFAULT RULE: All other traffic, use below proxies, in fai
```

在此示例PAC檔案中，首先生成DNS查詢，並將生成的IP捕獲到hostIP變量中。然後將生成的IP地址與每個Umbrella IP地址範圍進行比較。如果存在匹配項，則不會將查詢傳送到代理，而是直接傳送出去。如果沒有相符專案，則會將請求傳送到適當的代理。

請注意，對於未被阻止並因此未重定向到Umbrella IP地址的站點，使用以前的PAC檔案的效果是客戶端和代理都向遠端主機發出DNS請求。如果代理也使用OpenDNS，這意味著您的報告顯示重複的查詢。如果您使用的是虛擬裝置（如前所述），則可以通過為代理建立內部網路身份進行說明。如果需要，您可以為代理另外建立一個策略，完全禁用日誌記錄，以便隱藏這些重複請求。



附註：如果您在防火牆上阻止來自代理以外的源的出站HTTP/S請求，必須確保允許這些請求到達前面討論的IP範圍，以允許您的電腦訪問Umbrella阻止頁面。

透通代理

對於透明代理，HTTP流量在網路級別重新路由到Proxy。由於使用者端不知道代理，因此瀏覽器會生成自己的DNS請求。這表示如果代理也使用Umbrella，則每個請求都會重複。此外，由於代理使用它收到的DNS響應，而不是客戶端收到的結果，因此未正確應用策略。

與本文前面所述的明確情況不同，解決此問題不需要我們在客戶端上強制DNS請求，因為這種情況已經發生。但是，仍然需要將HTTP連線的Proxy旁路到Umbrella IP地址。執行此作業的方法差異很大，具體取決於您使用什麼機制將流量重新導向到Proxy。但是，一般來說，它涉及免除對Umbrella IP地址範圍進行重定向。

例如，假設在Cisco ASA上使用WCCP使用此ACL將流量重定向到Proxy:

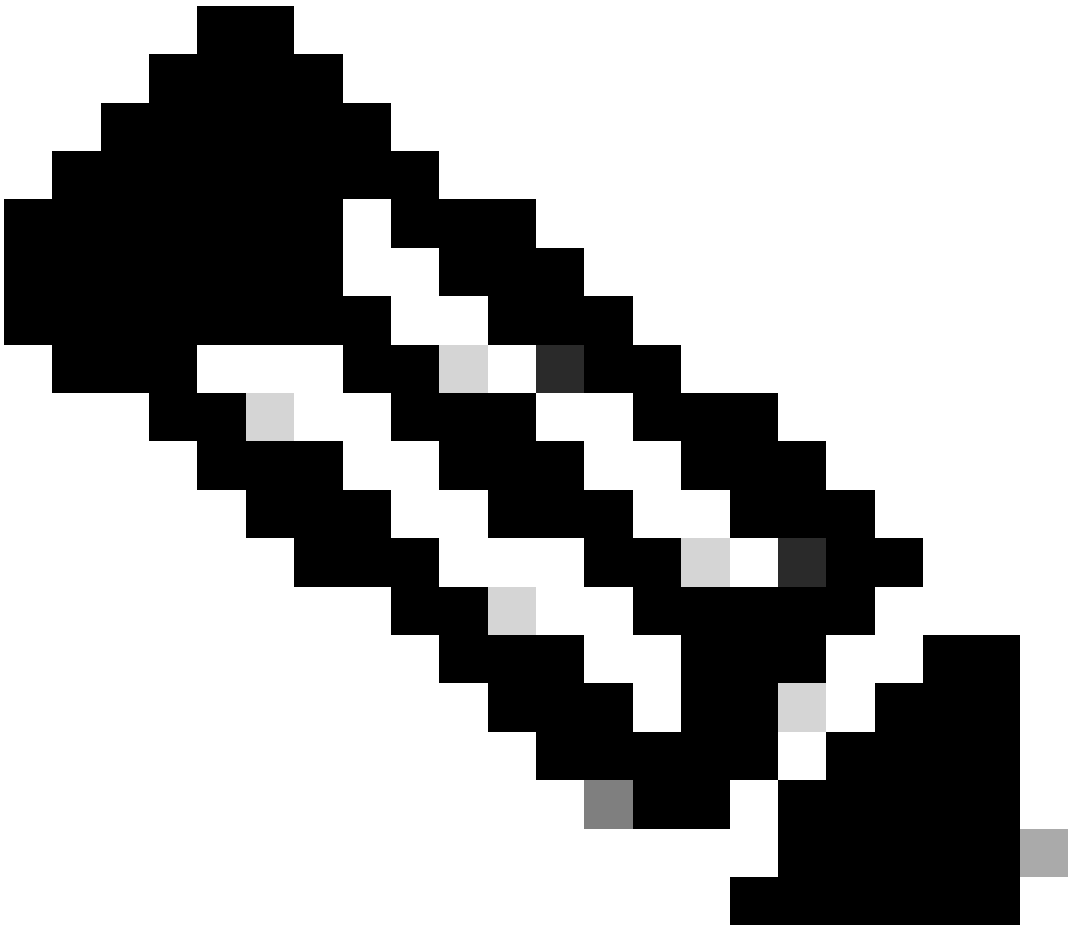
```
access-list wccp-traffic extended permit ip any any
```

可以修改wccp-traffic ACL以拒絕重新導向至Umbrella IP範圍的Proxy（從而繞過Proxy）：

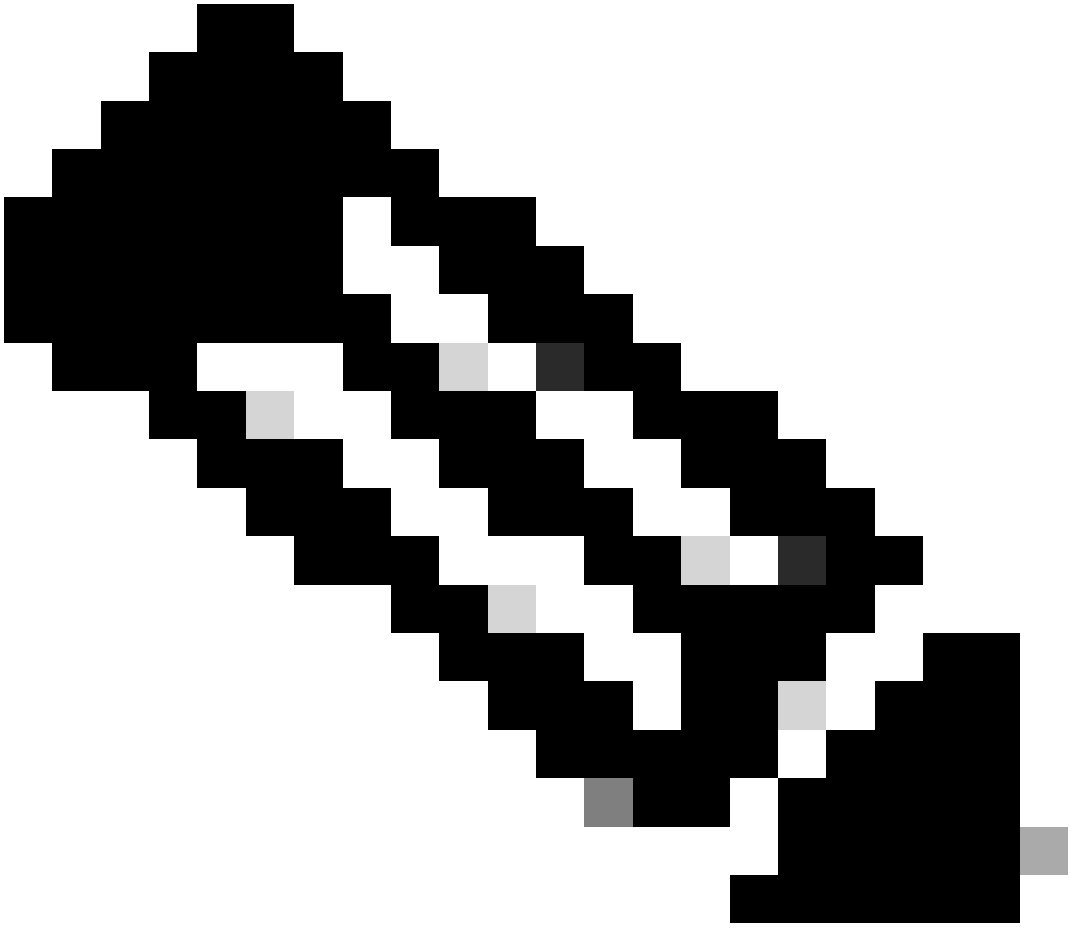
```
access-list wccp-traffic extended deny ip any 67.215.64.0 255.255.224.0access-list wccp-traffic extende
access-list wccp-traffic extended deny ip any 155.190.0.0 255.255.0.0
access-list wccp-traffic extended deny ip any 151.186.0.0 255.255.0.0



access-list wccp-traffic extended permit ip any any
```



附註：此ACL尚未經過測試，並且因使用的ASA版本或Cisco IOS®版本而異。請確保您建立的任何ACL都適合您的解決方案，並且在部署到生產環境之前已經過徹底測試。



附註：如果您在防火牆上阻止來自代理以外的源的出站HTTP/S請求，必須確保允許這些請求進入前面討論的IP範圍，以便允許您的電腦訪問Umbrella阻止頁。

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）。