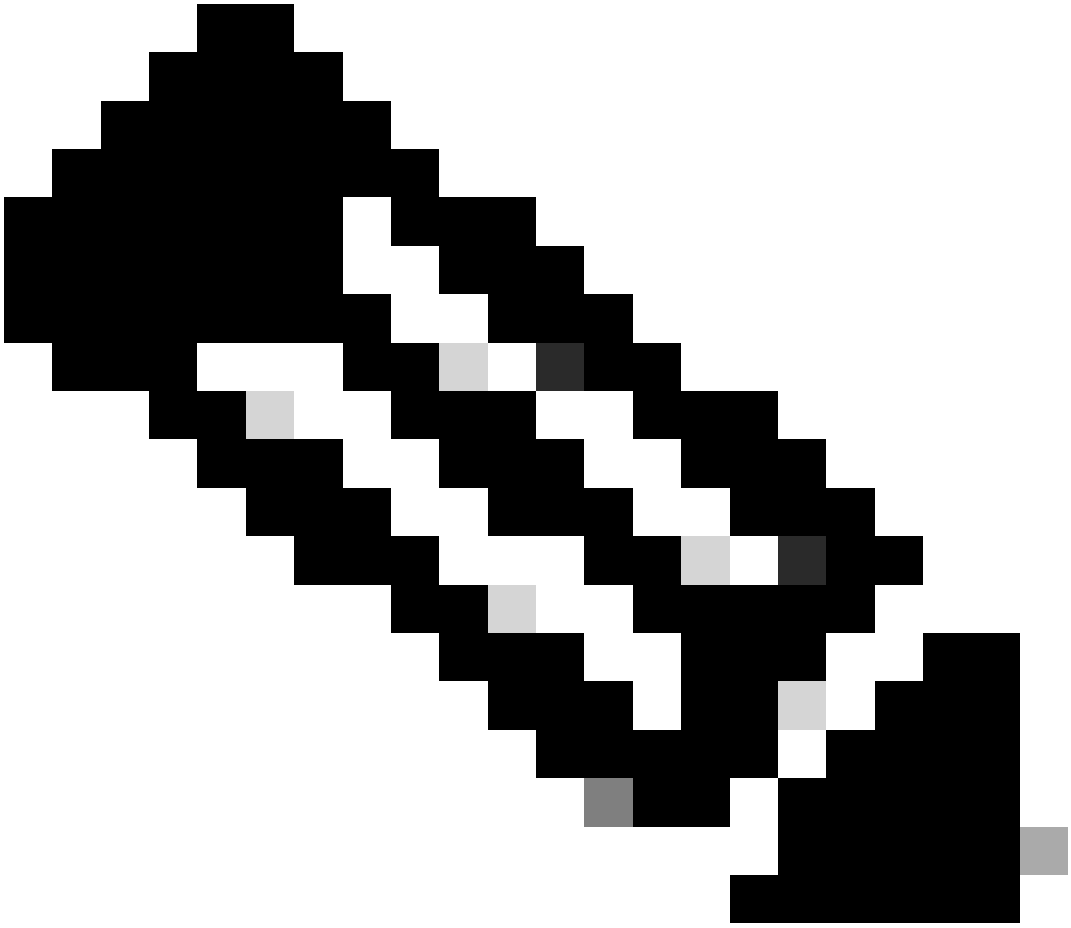
# 安全客戶端SWG模組中的外部域

## 目錄



## 簡介

本檔案將說明Cisco Secure Client(CSC)（前身為AnyConnect）安全Web閘道(SWG)模組如何套用已設定的外部網域清單及其影響。



附註：思科宣佈Cisco AnyConnect於2023年停用，Umbrella漫遊客戶端於2024年停用。許多Cisco Umbrella客戶已經從遷移到Cisco Secure Client中受益，我們鼓勵您儘快開始遷移，以獲得更好的漫遊體驗。閱讀此知識庫文章中的詳細資訊：如何在Umbrella模組中安裝Cisco Secure Client?

## 概觀

Cisco Umbrella External Domains list同時接受域和IP地址。但是，在這兩種情況下，CSC SWG模組只能基於IP地址應用排除決定。

在高級別，SWG模組用於識別流向外部域清單上的域的流量的機制如下：

- SWG模組監控來自客戶端電腦的DNS查詢，以識別外部域清單中的域的查詢
- 這些域及其對應的IP地址將新增到本地DNS快取
- 然後繞過SWG的決策會應用到任何發往與本地DNS快取中的外部域對應的IP的流量。決定不是基於HTTP請求中使用的域。

## 為什麼它是這樣運作的？

CSC SWG模組在第3層/第4層運行，因此它只能檢視儲存5元組連線詳細資訊（DestinationIP:Port、SourceIP:Port和Protocol）的TCP/IP報頭，其流量旁路規則可以基於這些報頭。

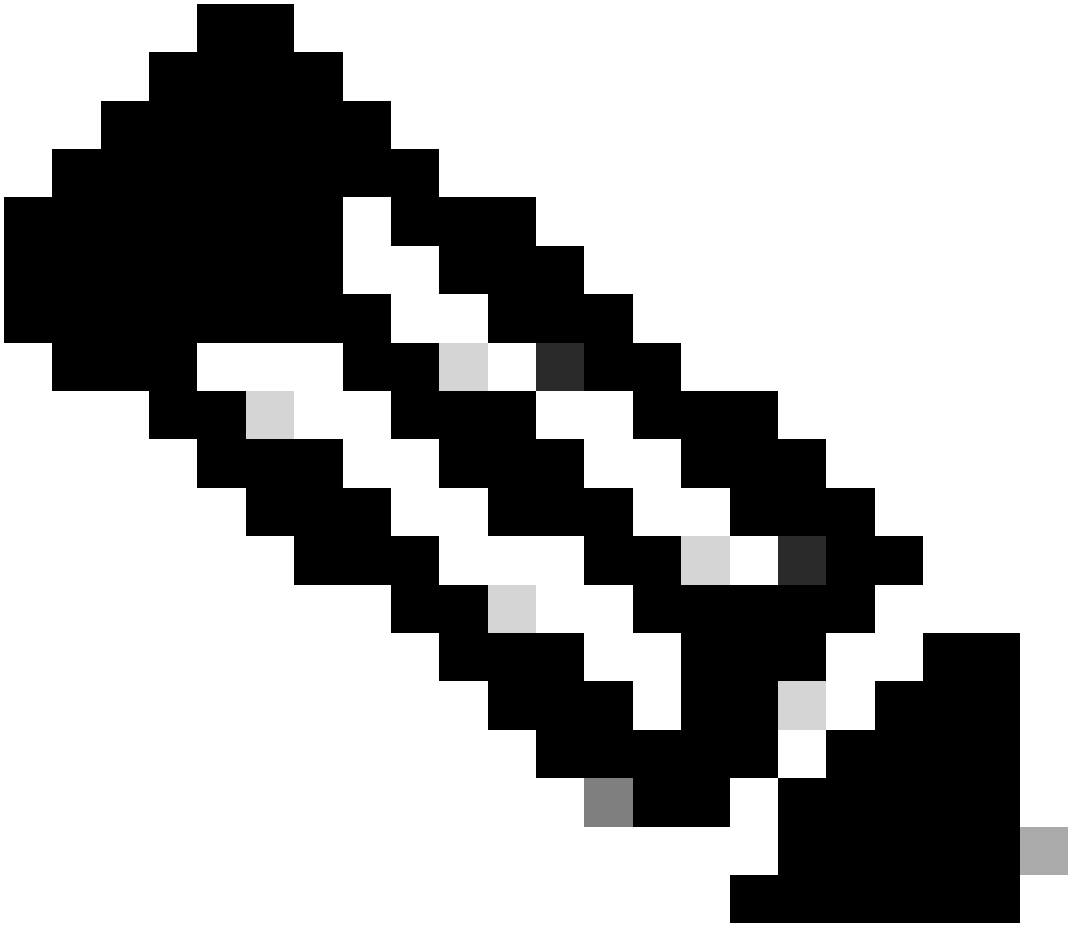
因此，對於基於域的旁路，CSC SWG需要將清單中的域轉換為IP地址，然後與客戶端電腦上的流量匹配。為此，它根據從客戶端傳送的DNS查詢生成DNS快取，DNS快取列出與外部域清單上的域對應的IP地址

然後，將繞過SWG的決策應用到攔截的流量（預設值為80/443），該流量將發往這些IP地址。

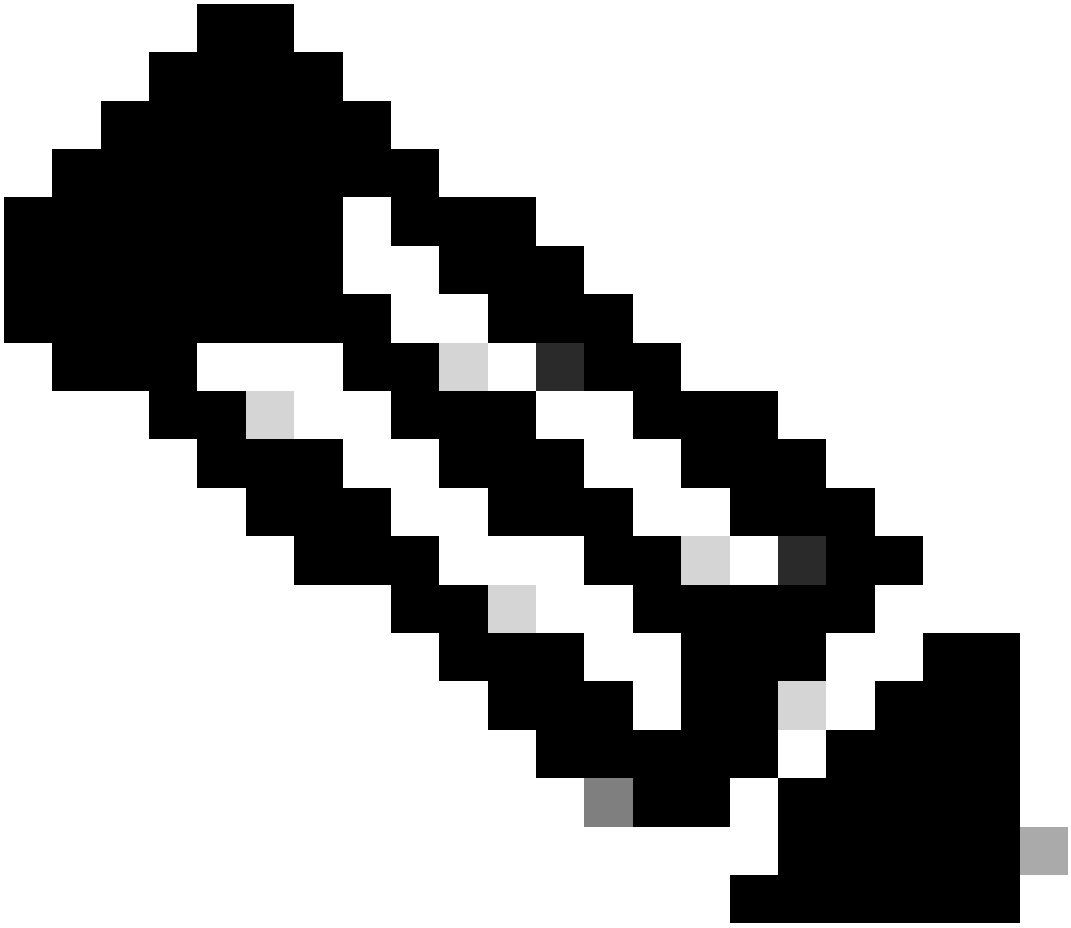
## 為什麼這對我來說很重要？

這可能導致幾個常見問題：

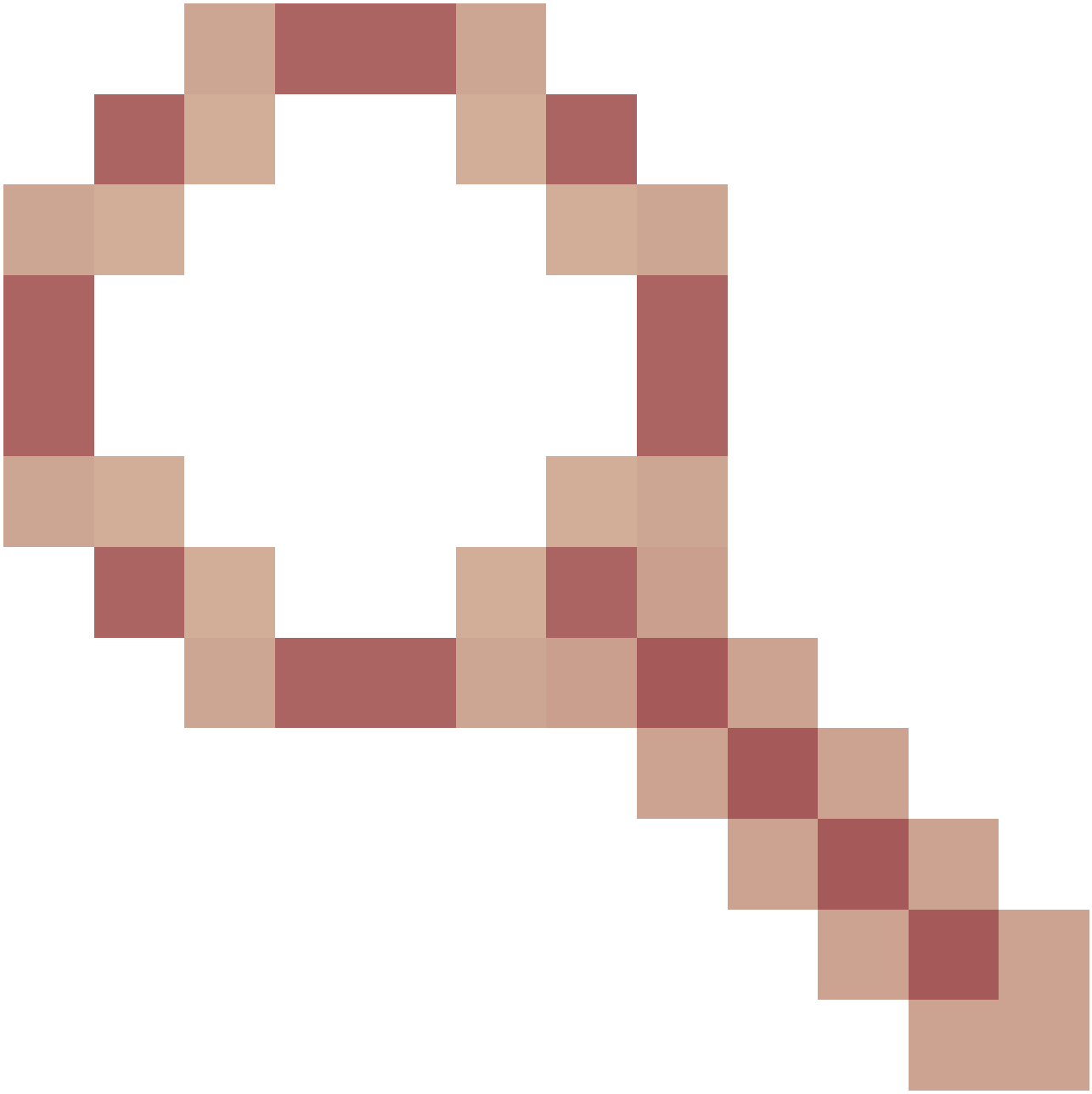
1. 由於繞行決策最終基於IP，因此共用同一IP的其他域的流量也會從Cisco Umbrella繞過，導致客戶觀察到直接從客戶端流入的意外流量，並且未應用或在活動搜尋中顯示SWG策略。
2. 如果由於任何原因，SWG模組無法看到該域的DNS查詢（如中的，該域有一個localhost條目），則不會將IP新增到快取，因此流量會意外傳送到SWG。



附註：KDF驅動程式僅監控UDP DNS查詢。如果由於任何原因通過TCP執行DNS查詢，則不會將IP新增到快取，也不會應用外部域。此資訊發佈在思科的Bug Search中。



附註：我們已修復了通過TCP解析DNS(CSCwe)時SWG模組外部域轉到Umbrella的48679題



)（Windows和MacOS），在Cisco Secure Client 5.1.4.74(MR4)中

## 如何對此流程進行故障排除？

SWG模組觀察DNS查詢、向DNS快取新增條目以及向發往IP的流量應用旁路操作的過程可以在KDF日誌中執行。這就要求啟用KDF日誌記錄，並且由於日誌的豐富性，只能在故障排除期間啟用較短時間。

### KDF日誌條目示例

要新增到DNS快取的域的DNS查詢：

```
00000283 11.60169029 acsock 11:34:57.9474385 (CDnsCachePluginImp::notify_recv): acquired safe buffer fo
00000284 11.60171318 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
```

```
00000285 11.60171986 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000286 11.60172462 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000287 11.60172939 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000288 11.60173225 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCache): Added entry (www.club386.com,
00000289 11.60173607 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
```

觀察到HTTPS連線，域不在外部域清單中，請求通過SWG傳送：

```
00000840 10.69207287 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): called
00000841 10.69207764 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00000842 10.69208336 acsock 12:13:50.0741618 (CSocketScanSafePluginImp::notify_bind): websec cookie FFF
00000843 10.69208908 acsock 12:13:50.0741618 (COpenDnsPluginImp::notify_bind): opendns cookie FFFFD30F9
00000844 10.69209576 acsock 12:13:50.0741618 (CNvmPlugin::notify_send): nvm: cookie 0000000000000000: pa
00000845 10.69211483 acsock 12:13:50.0741618 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by ad
00000846 10.69221306 acsock 12:13:50.0741618 (CSocketMultiplexor::notify_stream_v4): recv: protocol 6,
00000847 10.69222069 acsock 12:13:50.0741618 (CNvmPlugin::notify_recv): nvm: cookie 0000000000000000: pa
```

觀察到HTTPS連線，快取中找到IP條目，應用繞過操作：

```
00003163 9.63360023 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): called
00003164 9.63360405 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00003165 9.63360882 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_bind): websec cookie FFFF
00003166 9.63361359 acsock 15:33:48.7197706 (COpenDnsPluginImp::notify_bind): opendns cookie FFFF8C02C8
00003167 9.63364792 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): called
00003168 9.63365269 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): nvm: cookie 0x0000000000000000
00003169 9.63366127 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): websec cookie F
00003170 9.63367081 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003171 9.63367558 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003172 9.63370323 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::getFQDN_check_domain_exception):
00003173 9.63370800 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::evaluate_rules): domain name fou
00003174 9.63371372 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): cookie FFFF8C02
```

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）。