

對DNS活動日誌條目進行故障排除，判定已阻止

目錄

問題

報告以下一個或多個症狀：

- Activity Search (Monitor > Activity Search , 已過濾為DNS事件) 顯示域的Decision/Action = Blocked , 但是檢視Internet Access規則不會顯示明顯阻止該域的規則。
- 該域不存在於管理員維護的任何阻止目標清單中。

環境

- 本檔案中的資訊是根據：
 - 思科安全存取(SSE)雲平台
 - 具有漫遊安全模組的思科安全客戶端5.x已部署並註冊到安全訪問組織

解析

步驟1.驗證所評估的身份

- 確認決定針對哪個身份。如果事件顯示網路、站點或隧道標識而不是預期的漫遊電腦或使用者，則查詢匹配與所檢視的規則集不同的規則集。
- 對於漫遊使用者，驗證裝置是否已註冊並報告為受保護

標識不匹配：更正部署以便應用預期身份（註冊漫遊裝置、修復AD/使用者組對映或調整網路身份規則集），而不是鬆開不正確匹配的規則。

第2步：檢查安全類別是否匹配

- 如果事件包含安全類別（惡意軟體、C2、網路釣魚、新看見的域、DNS隧道等），則阻止來自匹配規則集的安全設定 — 沒有目標清單或內容規則需要引用該域。
- 在Cisco Talos情報門戶上查詢域的當前信譽和分類，網址為<https://talosintelligence.com/>（信譽中心查詢）。
- 如果Talos中顯示的分類或信譽不正確，請直接通過<https://talosintelligence.com/>向Talos提交爭議/重新分類請求（提交案例），以便重新評估該域。Talos更新分類後，更改將傳播到安全訪問實施。

步驟3：檢查CNAME鏈

- 從未篩選的有利點解析域並檢查整個應答鏈(例如，`dig +noall +answer <domain>`或`nslookup -debug <domain>`)。
- 根據目標清單和Talos分類檢查鏈中的每個CNAME目標；受阻的CNAME目標解釋對顯然乾淨的查詢域所做的受阻決策

第4步：重新自上而下評估策略的實際身份

- 從步驟1開始，按照身份順序瀏覽Internet訪問規則，檢查每個規則的身份範圍、計畫、已啟用狀態以及安全/內容/應用程式設定，一直到預設規則並包括預設規則。
- 使用具有準確身份和目的地的策略測試程式(例如 — policy.test.sse.cisco.com/?=cisco.com)檢視哪個規則Secure Access報告為匹配項，並將其與事件上命名的規則進行比較。

特殊情況：新發現的域

如果事件的安全類別是Newly Seen Domains(NSD)

補救選項（按優先順序排列）：

如果域對於業務至關重要，請將其新增到允許適用規則引用的目標清單；對於該目標，allow條目優先於NSD安全塊。

禁用加密的DNS(DoH)和QUIC

加密的DNS和QUIC可能導致導致DNS層可見性差距，從而導致活動搜尋結果混亂：通過瀏覽器DoH解決的查詢從未到達安全訪問解析器（因此它們完全不在日誌中），而DoH提供程式域本身可能顯示為「已阻止」事件。

在受管端點上禁用這些傳輸可確保所有DNS保持可檢查狀態，活動日誌反映實際端點行為。

每個瀏覽器的HTTPS上的DNS(DoH)

Google Chrome

- 手動：導覽至chrome://settings/security，然後關閉使用安全DNS。

Microsoft Edge

- 手動：導覽至edge://settings/privacy，然後關閉使用安全DNS。

Mozilla Firefox

- 手動：Menu > Settings > Privacy & Security > DNS over HTTPS（或較舊版本中的網路設定），然後選擇Off/取消選擇Enable DNS over HTTPS。
- 附註：Umbrella/Secure Access解析器以向Firefox發出訊號，在預設情況下保持DoH關閉的方式回應Mozilla canary域(use-application-dns.net)；仍建議使用顯式GPO設定，因為使用者設定的DoH配置會覆蓋金絲雀檢查。注意：請勿將Mozilla kill-switch/canary域新增到塊目標清單——塊頁A記錄響應被視為有效，並且可能導致Firefox保留或升級其DoH使用情況。

QUIC(HTTP/3)

QUIC在UDP/443上運行，可以傳輸一般的Web流量和DoH3(DNS over HTTP/3)，繞過預期為TCP的檢查路徑。

禁用QUIC會強制瀏覽器回退到基於TCP的HTTP/2或HTTP/1.1，從而恢復完全可視性：

- Chrome/Edge:手動 (非永續性，使用者可更改)：將chrome://flags/#enable-quic / edge://flags/#enable-quic設定為Disabled。
- Firefox:設定首選項network.http.http3.enable = false(about:config or policy/AutoConfig)。

如果在這些步驟之後，事件上報告的匹配規則仍無法與配置協調，請與Cisco TAC建立案例，並提供活動搜尋事件匯出 (時區時間戳、身份、匹配規則、類別、記錄型別和域) 以及相關規則和目標清單的螢幕截圖。

原因

安全類別匹配 (Talos智慧) — 域被基於思科Talos信譽和分類 (而不是管理員明確配置的任何目標清單或內容規則) 的安全設定(例如Malware、Command and Control、Phishing、Cryptomining、DNS Tunneling或Newly Seen Domains)阻止。這是「無明顯匹配」塊的最常見原因。

身份屬性不匹配 — 查詢歸因於與預期不同的身份 (網路/站點身份而不是漫遊電腦、不同的AD使用者/組，或者未註冊裝置回退到網路級別的策略)，因此匹配了不同的規則 (通常更嚴格或預設)。

規則順序和預設規則 — 策略中更高級的規則 (或底部的預設/捕獲全部規則) 與預期的Allow規則匹配；目標規則也可以被禁用、計畫或限定到不包括受影響源的標識。

目標清單繼承 — 阻止目標清單包含父域(example.com)，該父域隱式覆蓋所有子域(app.example.com)，或包含域解析到的IP/CIDR。僅搜尋清單以查詢準確的FQDN不會顯示這一點。

CNAME鏈封鎖 — 允許查詢的域，但其解析鏈包含到被封鎖的域 (通常是CDN、追蹤器或駐留/封鎖主機) 的CNAME;該決策將應用於該鏈，並且日誌將原始查詢域顯示為Blocked。

應用程式或內容類別匹配 — 域屬於被阻止的應用程式 (應用程式控制元件) 或管理員未與之關聯的內容類別；分類可能與直覺不同 (例如，分類為檔案共用或代理/匿名程式的業務工具)。

最近策略或分類更改 — 策略或Talos分類最近發生更改；正在稽核的事件早於 (或遲於) 更改，或者策略傳播/客戶端同步在查詢時尚未完成。

相關內容

- [為Umbrella配置內部DNS伺服器](#)
- [使用Umbrella設定透過HTTPS\(DoH\)的DNS](#)
- [在安全訪問中新增域控制器](#)
- [Cisco Secure Access Block頁面資訊](#)
- [思科技術支援與下載](#)

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）。