使用GREP過濾訪問日誌

目錄

問題：

環境:思科網路安全裝置(WSA),AsyncOS的所有版本

如何搜尋S系列裝置上的訪問日誌？

從思科網路安全裝置的命令列介面，可以使用**grep**命令來過濾訪問日誌並確定被阻止的內容。以下範例顯示所有遭封鎖的專案：

```
----------------------------------------
TestS650.wsa.com()> grep

當前配置的日誌：
1."accesslogs"型別：「訪問日誌」檢索：FTP輪詢
<..>
18. "welcomeack_logs"型別："歡迎頁面確認日誌"
檢索：FTP輪詢

輸入要記錄的日誌編號。
[]> 1

輸入正規表示式以grep。
[]> BLOCK_

是否希望此搜尋不區分大小寫？[Y]>n

是否要跟蹤日誌？[N]> n

是否要對輸出進行分頁？[N]> n

（將顯示條目）
----------------------------------------
```

對於正規表示式問題，可以輸入**BLOCK_**（不帶引號）以顯示WSA已阻止的每個請求。(警告:此清單可能很長)。

如果要顯示與特定站點相關的訪問長條目，還可以輸入站點URL的一部分。例如 — 為正規表示式輸入**windowsupdate**將顯示包含windowsupdate.microsoft.com的Windows Update URL的所有訪問日誌條目。

如果想要在URL中顯示windowsupdate的站點的訪問日誌條目（該條目也被阻止），則可以使用正規表示式 windowsupdate.*BLOCK_。