排除與主機防火牆的惡意連線故障

目錄

簡介

本文檔介紹如何在Windows終端上檢測惡意連線，並使用Cisco安全終端中的主機防火牆阻止它們。

必要條件

需求

- Host Firewall隨Secure Endpoint Advantage和Premier軟體包提供。
- 支援的聯結器版本
  - Windows(x64):安全終端Windows聯結器8.4.2及更高版本。
  - Windows(ARM):安全終端Windows聯結器8.4.4及更高版本。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

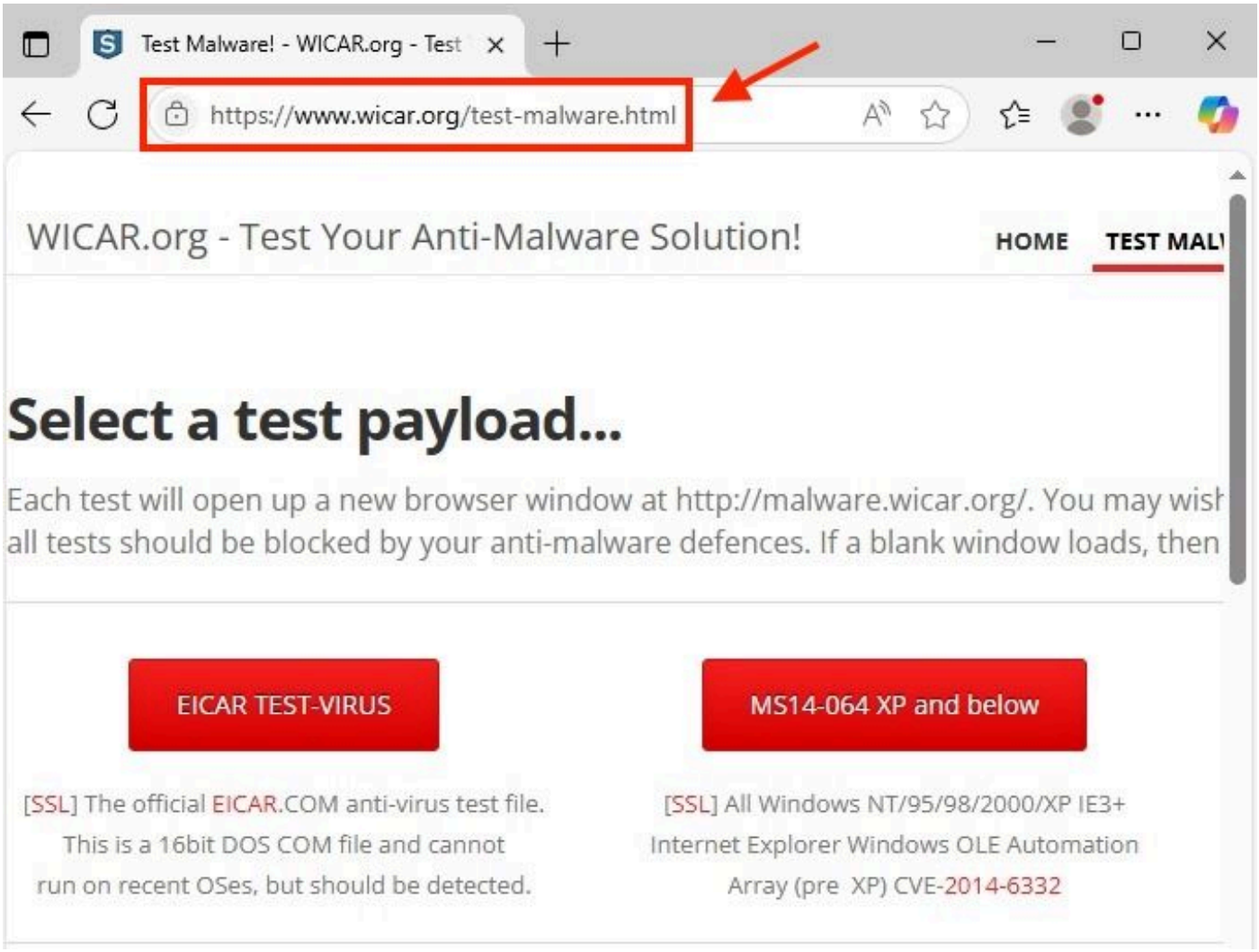
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解指南

本文檔提供使用思科安全終端主機防火牆阻止惡意連線的指南。為了進行測試，請使用測試頁malware.wicar.org(208.94.116.246)建立故障排除指南。

識別和阻止惡意連線的步驟

1. 首先，您需要確定要檢視和阻止的URL或IP地址。對於此案例，請訪問consider malware.wicar.org。
2. 驗證是否對該URL的訪問方式為successful. malware.wicar.org，且重新導向到其他URL，如圖所示。



瀏覽器惡意URL

3.使用nslookup命令檢索與URL malware.wicar.org關聯的IP地址。

```
C:\Users\Administrator>nslookup malware.wicar.org
Server:  dns-nextengo
Address:  10.2.9.164

Non-authoritative answer:
Name:    wicarmalware.nfshost.com
Addresses:  2607:ff18:80:6::6a08
          208.94.116.246
Aliases:  malware.wicar.org
```

nslookup輸出

4.一旦獲取惡意IP地址，請使用命令netstat -ano檢查終端上的活動連線。

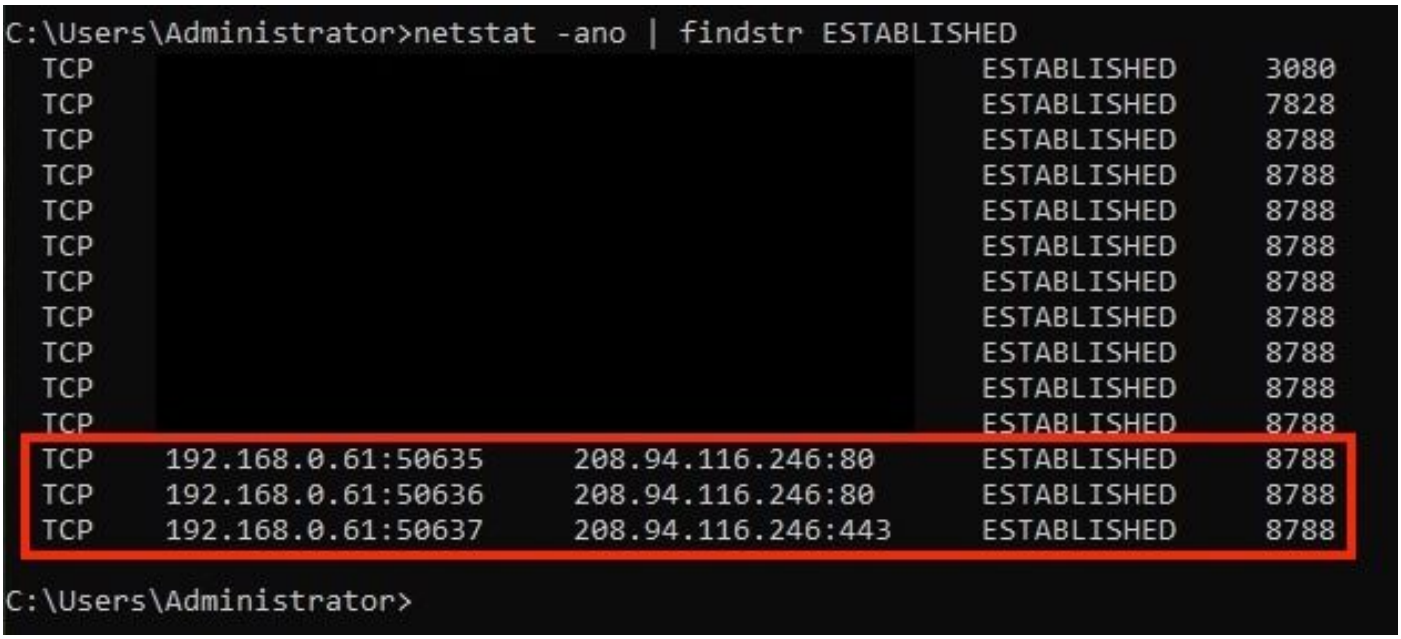
```
C:\Users\Administrator>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5140
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       7820
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       788
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       664
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1600
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1580
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2764
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       736
  TCP                                                  LISTENING       4
  TCP                                                  ESTABLISHED     3080
  TCP                                                  ESTABLISHED     7828
  TCP                                                  CLOSE_WAIT      5056
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  CLOSE_WAIT      5056
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP                                                  ESTABLISHED     8788
  TCP    192.168.0.61:50635     208.94.116.246:80      ESTABLISHED     8788
  TCP    192.168.0.61:50636     208.94.116.246:80      ESTABLISHED     8788
  TCP    192.168.0.61:50637     208.94.116.246:443     ESTABLISHED     8788
  TCP    [::]:135               [::]:0                 LISTENING       492
  TCP    [::]:445               [::]:0                 LISTENING       4
```

所有連線的netstat

5.為了隔離活動連線，請應用過濾器以僅顯示已建立的連線。



用於已建立連線的netstat

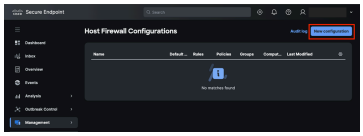
6.在上一個輸出中查詢從thenslookupcommand獲取的IP地址。確定源IP、目的IP、源埠和目的埠。

- 本地IP:192.168.0.61
- 遠端IP:208.94.116.246
- 本地埠：不適用
- 目的地埠80和443

7.收到此資訊後，導航到思科安全終端門戶以建立主機防火牆配置。

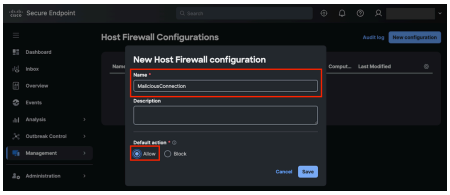
主機防火牆配置和規則建立

1. 導覽至Management > Host Firewall，然後單擊New Configuration。

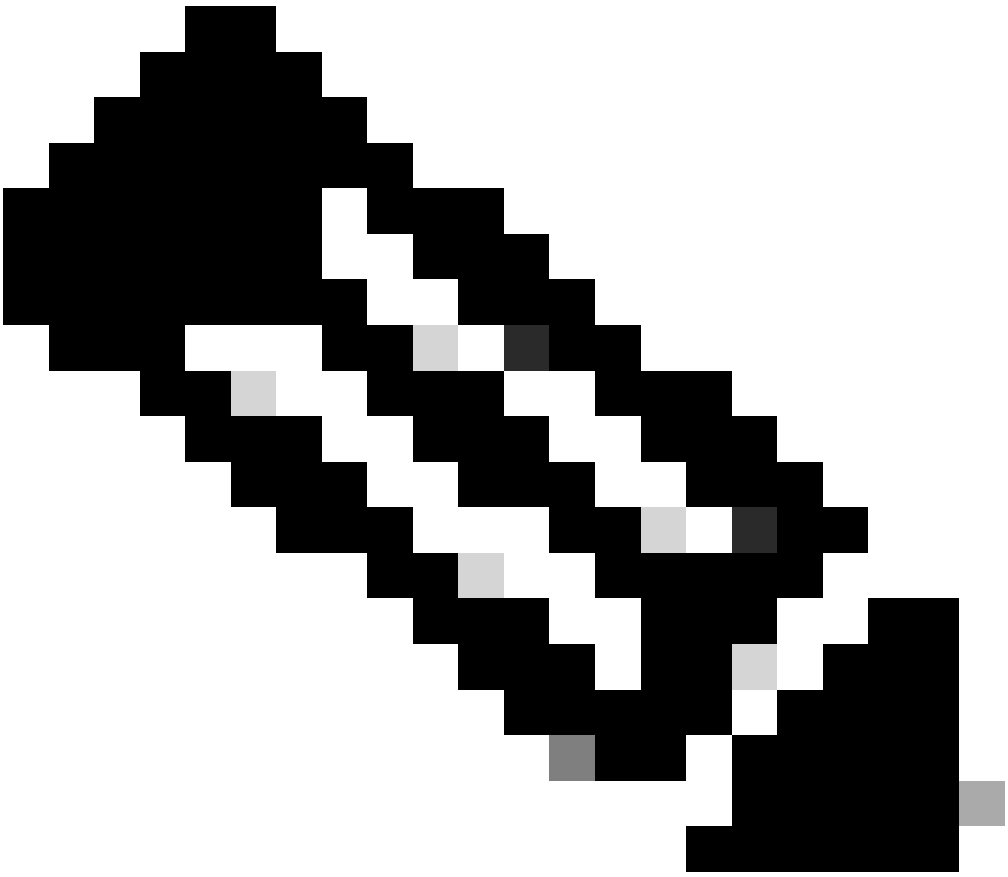


主機防火牆新配置

2. 選擇名稱和Default Action。在這種情況下，請選擇「允許」。

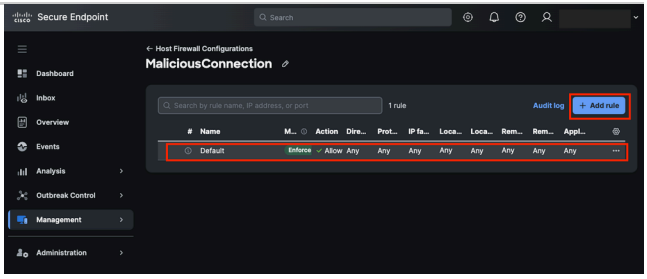


主機防火牆配置名稱和預設操作



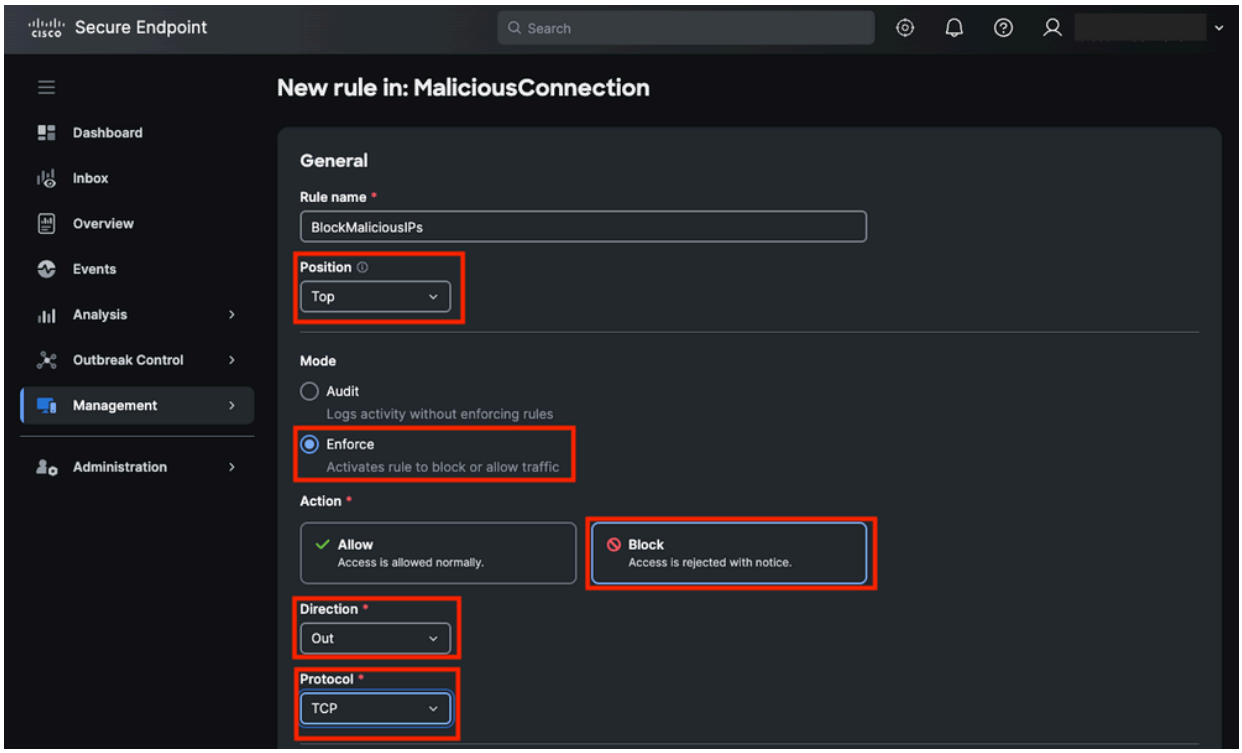
附註：請記住，您建立了一個阻止規則，但必須允許其他流量避免對合法連線產生影響。

3. 驗證是否已建立預設規則，然後單擊Add Rule。

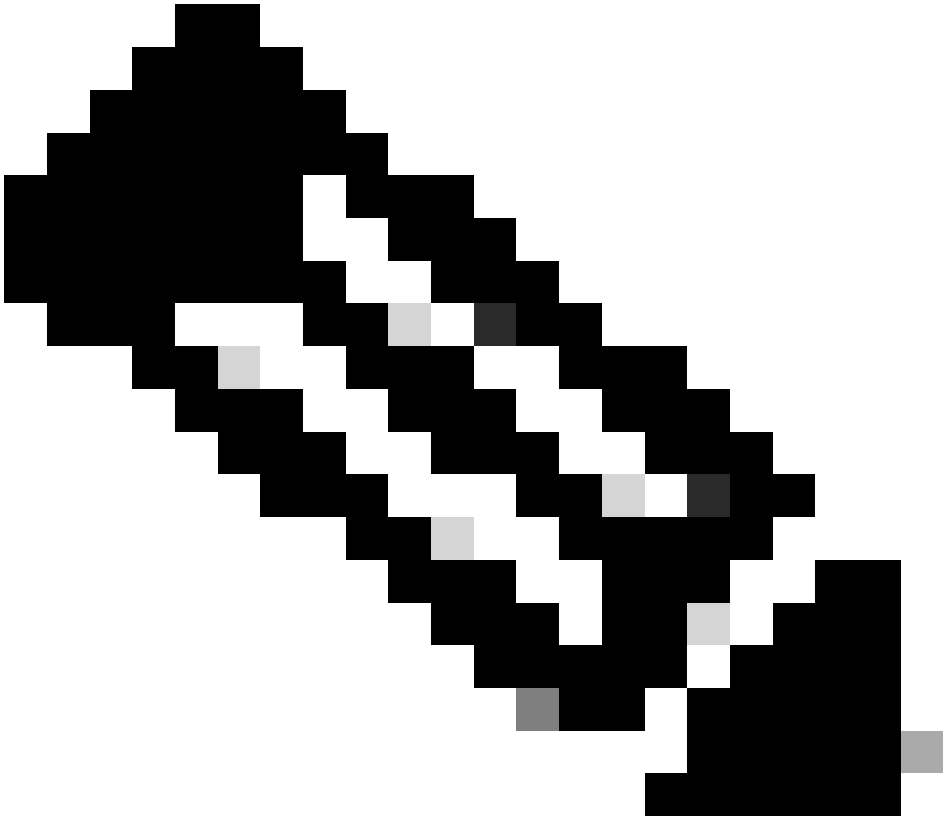


在主機防火牆中新增規則

4. 分配名稱並設定下一個引數：
   - 位置:頂端
   - Mode:實施
   - Action:封鎖
   - Direction:外寄
   - 通訊協定：TCP

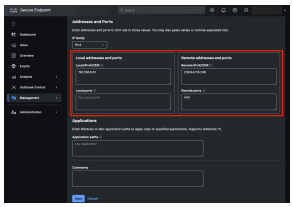

Secure Endpoint
Search
Dashboard
Inbox
Overview
Events
Analysis
Outbreak Control
Management
Administration
New rule in: MaliciousConnection
General
Rule name *
BlockMaliciousIPs
Position
Top
Mode
Audit
Logs activity without enforcing rules
Enforce
Activates rule to block or allow traffic
Action *
Allow
Access is allowed normally.
Block
Access is rejected with notice.
Direction *
Out
Protocol *
TCP

規則常規引數



附註：當您處理從內部終端到外部目標（通常是Internet）的惡意連線時，方向始終為Out。

5. 指定本地和目標IP:
    - 本地IP:192.168.0.61
    - 遠端IP:208.94.116.246
    - 將Local Portfield留空。
    - 將Destination埠設定為80和443，這兩個埠對應於HTTP和HTTPS。

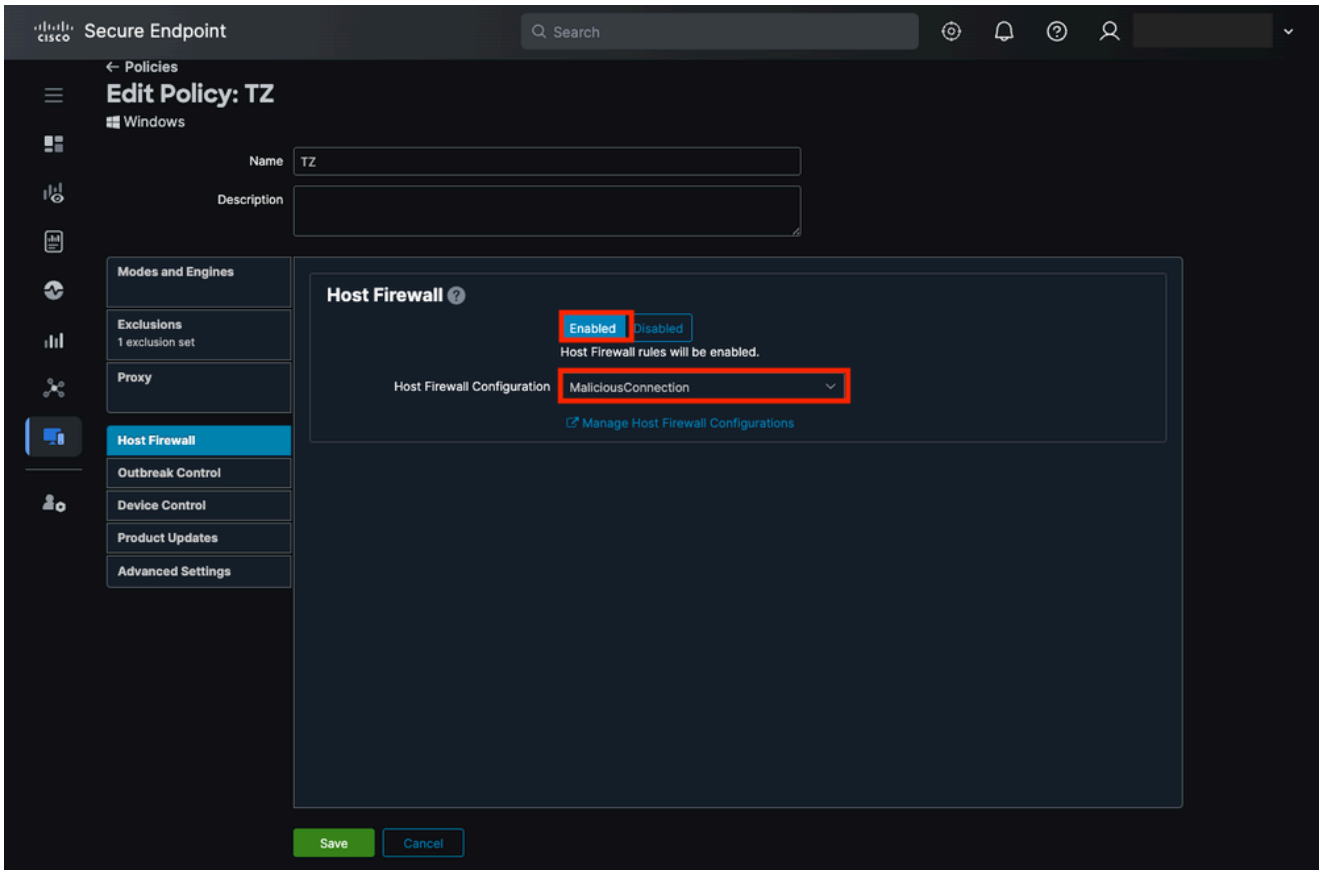


規則地址和埠

6.最後，按一下「儲存」。

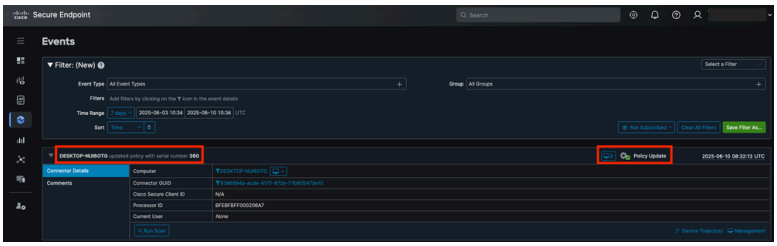
在策略中啟用主機防火牆並分配新配置

1. 在安全終端門戶中，導航到管理>策略，然後選擇與要阻止惡意活動的終端關聯的策略。
2. 按一下編輯並導航到主機防火牆頁籤。
3. 啟用Host Firewall功能並選擇最近的配置，本例中為MaliciousConnection。



在安全端點策略中啟用主機防火牆

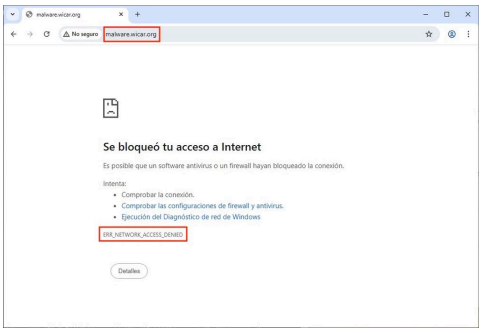
4. 按一下「Save」。



5. 最後，驗證終端是否已應用策略更改。

策略更新事件

在本地驗證配置



1. 在瀏覽器中使用URL malware.eicar.org，確認它已被阻止。

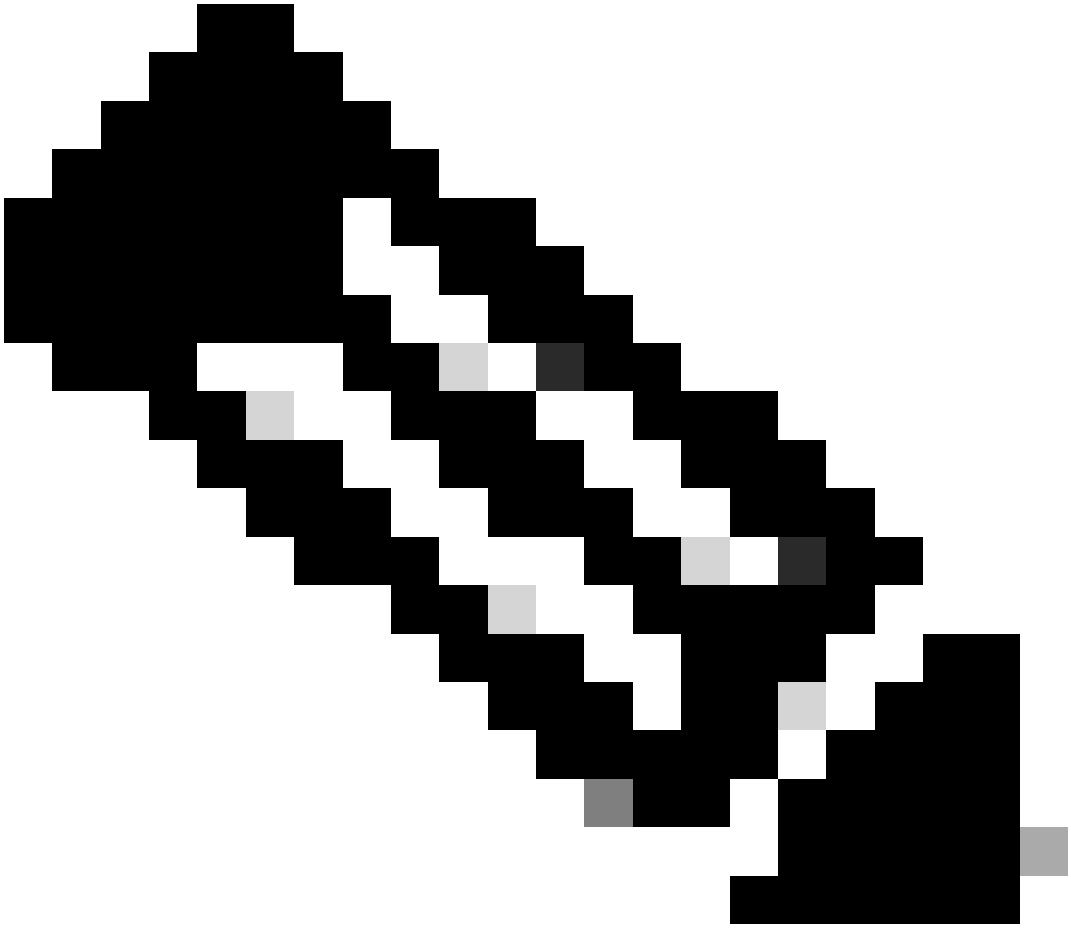
錯誤：拒絕從瀏覽器訪問網路

2. 確認該塊後，驗證是否未建立連線。使用命令netstat -ano | findstr ESTABLISHED以確保與惡意URL(208.94.116.246)關聯的IP不可見。

檢視日誌

1.在終端上，導航到資料夾:

C:\Program Files\Cisco\AMP\<聯結器版本>\FirewallLog.csv



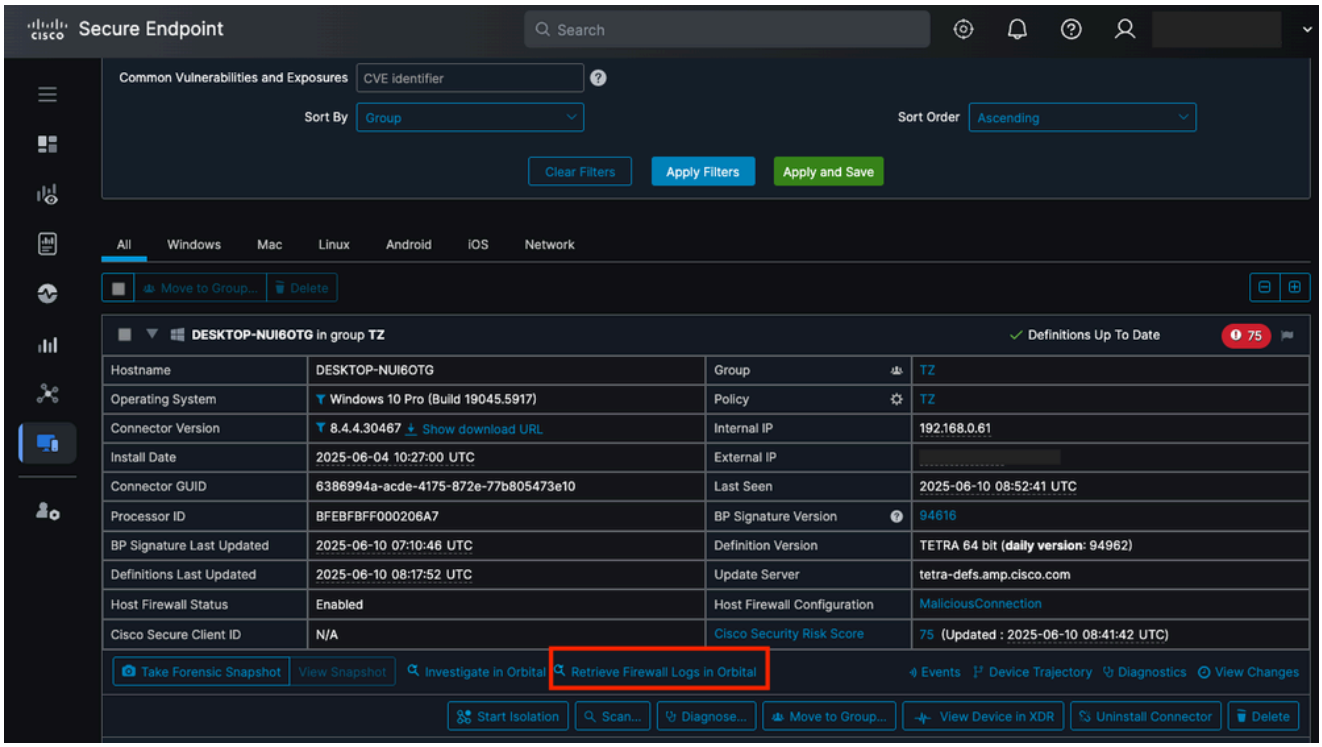
附註：日誌檔案位於<安裝目錄>\Cisco\AMP\<Connector version>\FirewallLog.csv資料夾中

2.開啟CSV檔案以驗證「阻止」操作規則的匹配項。使用過濾器區分「允許」和「阻止」連線。

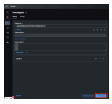
CSV檔案中的防火牆日誌

使用Orbital檢索防火牆日誌

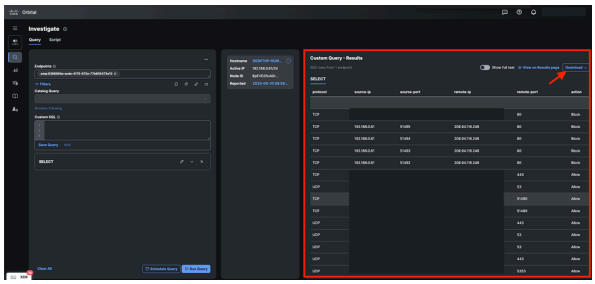
1. 在Secure Endpoint Portal中，導航到Management > Computers，找到終端，然後按一下Retrieve Firewall Logs in Orbital。此操作會將您重定向至軌道門戶。



用於在軌道中檢索防火牆日誌的按鈕

2. 在Orbital Portal中，點選運行查詢。此操作顯示記錄在主機防火牆端點上的所有日誌。 

從軌道運行查詢

3. 該資訊在Resultstab中可見，您也可以下載該資訊。 

軌道查詢結果

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）。