排除与主机防火墙的恶意连接故障

目录

简介

本文档介绍如何使用Cisco安全终端中的主机防火墙检测Windows终端上的恶意连接并阻止它们。

先决条件

要求

- 主机防火墙可与Secure Endpoint Advantage和Premier软件包配合使用。
- 支持的连接器版本
  - Windows(x64):保护终端Windows连接器8.4.2及更高版本。
  - Windows(ARM):保护终端Windows连接器8.4.4及更高版本。

使用的组件

本文档不限于特定的软件和硬件版本。

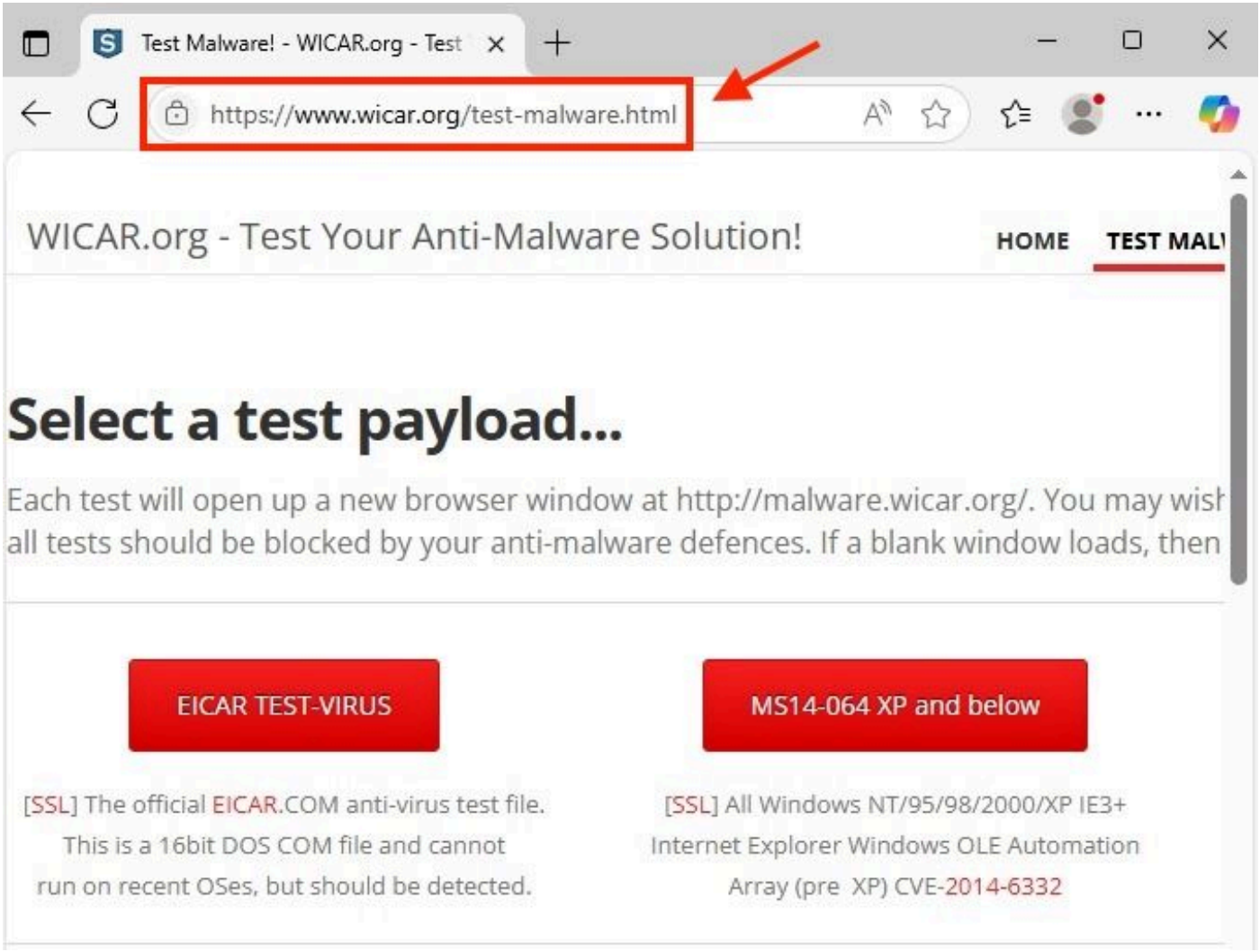
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除指南

本文档提供使用思科安全终端主机防火墙阻止恶意连接的指南。为了进行测试，请使用测试页malware.wicar.org(208.94.116.246)创建故障排除指南。

识别并阻止恶意连接的步骤

1. 首先，您需要确定要查看和阻止的URL或IP地址。对于此场景consider malware.wicar.org。
2. 验证对URL的访问是否为successful. malware.wicar.org重定向到其他URL，如图所示。



浏览器恶意URL

3.使用nslookup命令检索与URL malware.wicar.org关联的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输出

4.一旦获取恶意IP地址，请使用命令netstat -ano检查终端上的活动连接。

```
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                                                  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
```

所有连接的netstat

5.为了隔离活动连接，请应用过滤器以仅显示已建立的连接。

```
C:\Users\Administrator>netstat -ano | findstr ESTABLISHED
  TCP                                                    ESTABLISHED     3080
  TCP                                                    ESTABLISHED     7828
  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

C:\Users\Administrator>
```

已建立连接的netstat

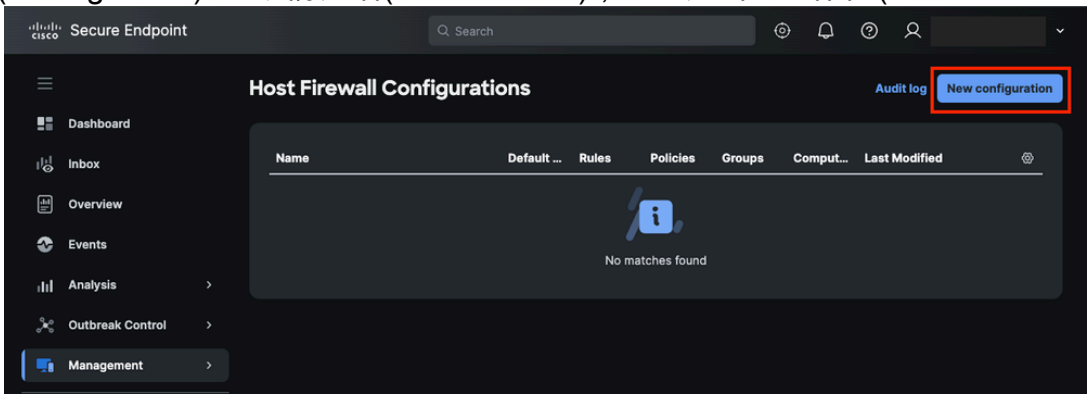
6.在上一输出中查找从thenslookupcommand获取的IP地址。确定源IP、目标IP、源端口和目标端口。

- 本地 IP:192.168.0.61
- 远程 IP:208.94.116.246
- 本地端口:不能应用
- 目的端口到80和443

7.获得此信息后，导航到Cisco Secure Endpoint Portal以创建主机防火墙配置。

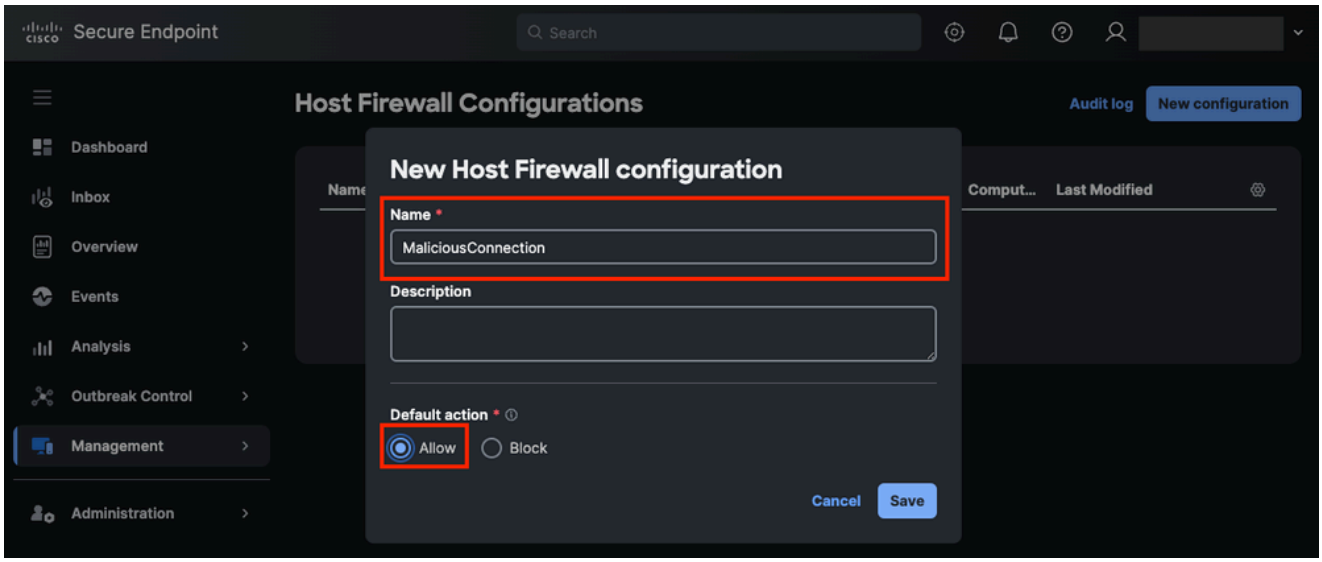
主机防火墙配置和规则创建

1. 依次导航到管理(Management)>主机防火墙(Host Firewall)，然后点击新建配置(New Configuration)。

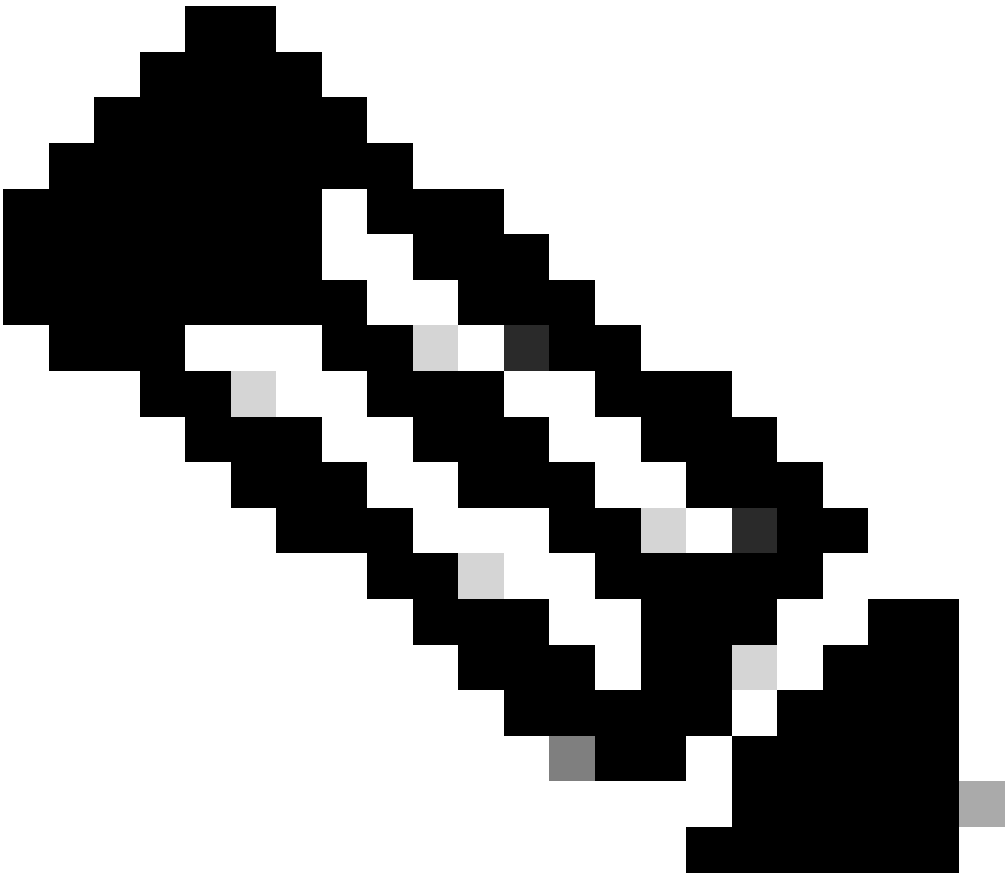


主机防火墙新配置

2. 选择name和Default Action。在本例中，选择允许。

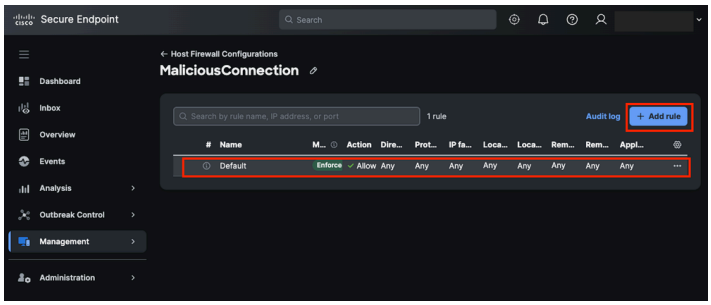


主机防火墙配置名称和默认操作



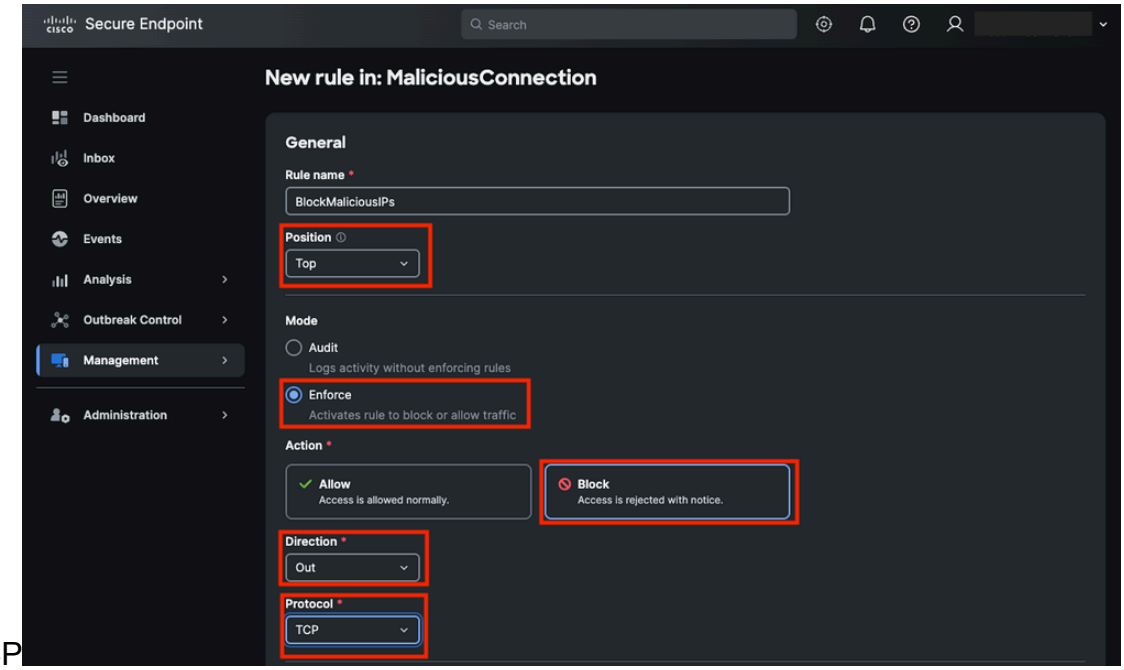
注意：请记住，您创建了一个阻止规则，但必须允许其他流量以免影响合法连接。

3. 确认已创建默认规则，然后点击Add Rule。

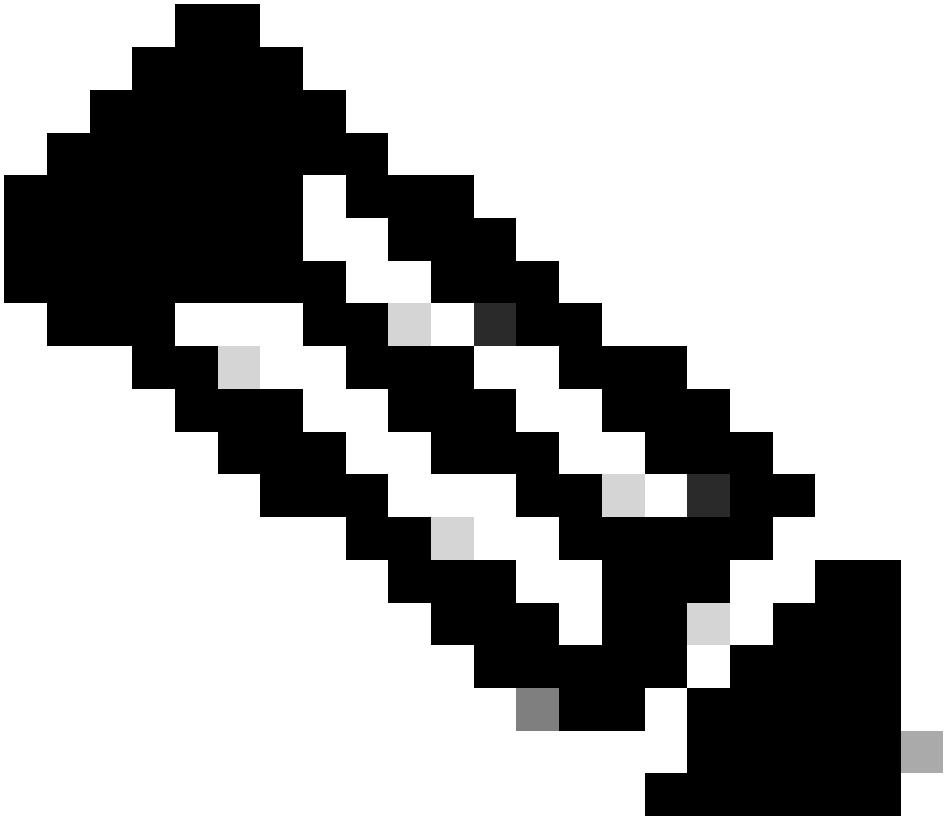


在主机防火墙中添加规则

4. 指定名称并设置下一个参数：
   - 位置:顶部
   - 模式:实施
   - 操作：阻止
   - 方向:出站
   - 协议:TCP

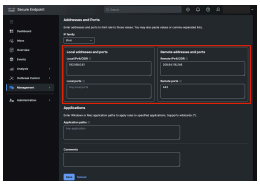


规则常规参数



注意：当您处理从内部终端到外部目标（通常是Internet）的恶意连接时，方向始终为Out。

5. 指定本地和目标IP:
   - 本地 IP:192.168.0.61
   - 远程 IP:208.94.116.246
   - 将Local Portfield留空。
   - 将Destination端口设置为80和443，这些端口对应于HTTP和HTTPS。



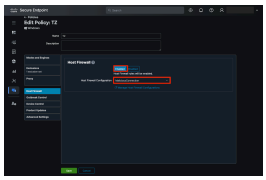
规则地址和端口

6.最后，单击保存。

在策略中启用主机防火墙并分配新配置

1. 在安全终端门户中，导航到Management > Policies，然后选择与要阻止恶意活动的终端关联的策略。
2. 点击编辑(Edit)并导航到主机防火墙(Host Firewall)选项卡。

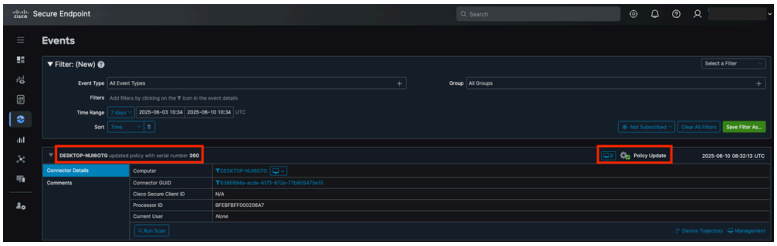
3. 启用Host Firewall功能并选择最近的配置，本例中为MaliciousConnection。



在安全终端策略中启用主机防火墙

4. Click Save.

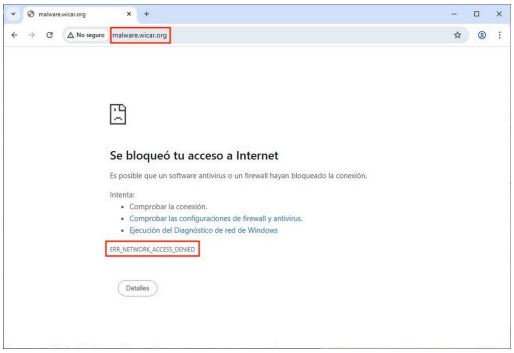
5. 最后，验证终端是否已应用策略更改。



策略更新事件

本地验证配置

1. 在浏览器中使用URL malware.eicar.org确认其已被阻止。



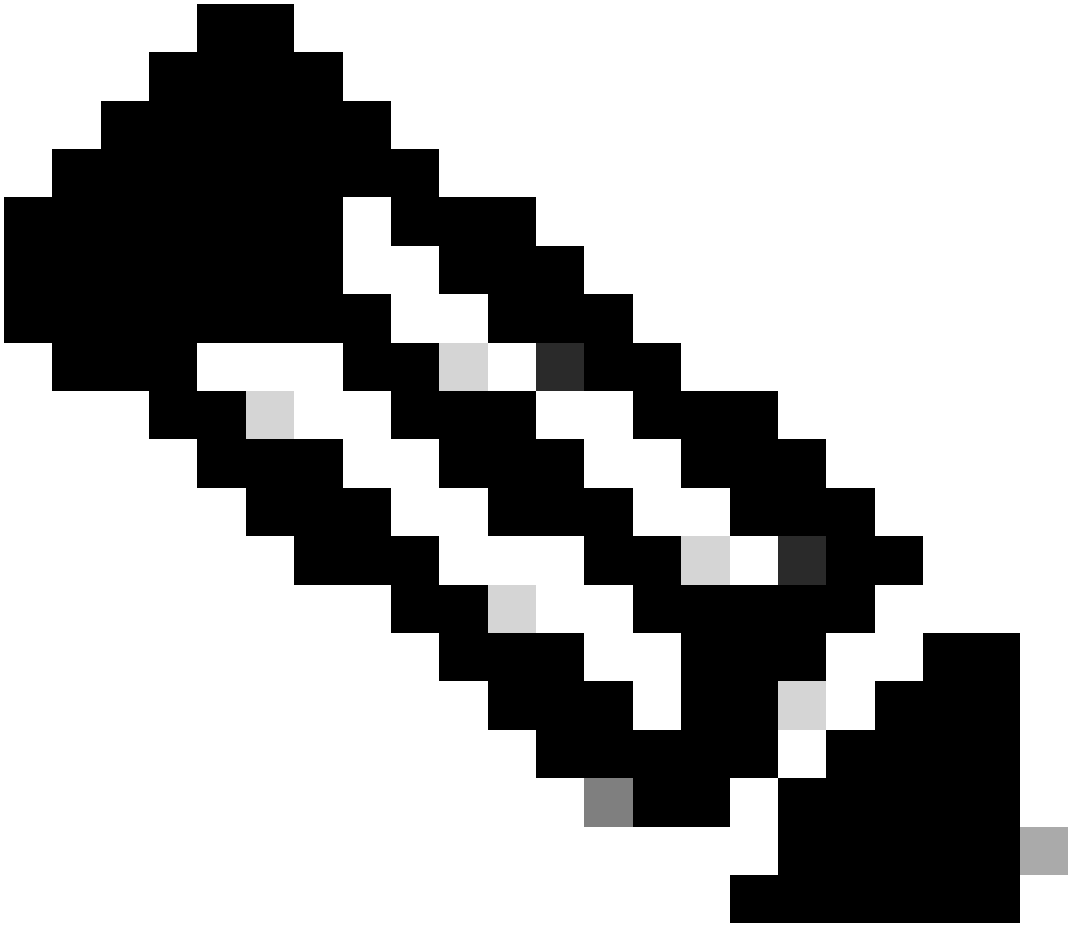
错误：拒绝从浏览器访问网络

2. 确认阻止后，验证未建立连接。使用命令netstat -ano | findstr ESTABLISHED可确保与恶意URL(208.94.116.246)关联的IP不可见。

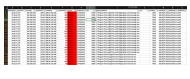
审核日志

1.在终端上，导航到文件夹:

C:\Program Files\Cisco\AMP\<连接器版本>\FirewallLog.csv



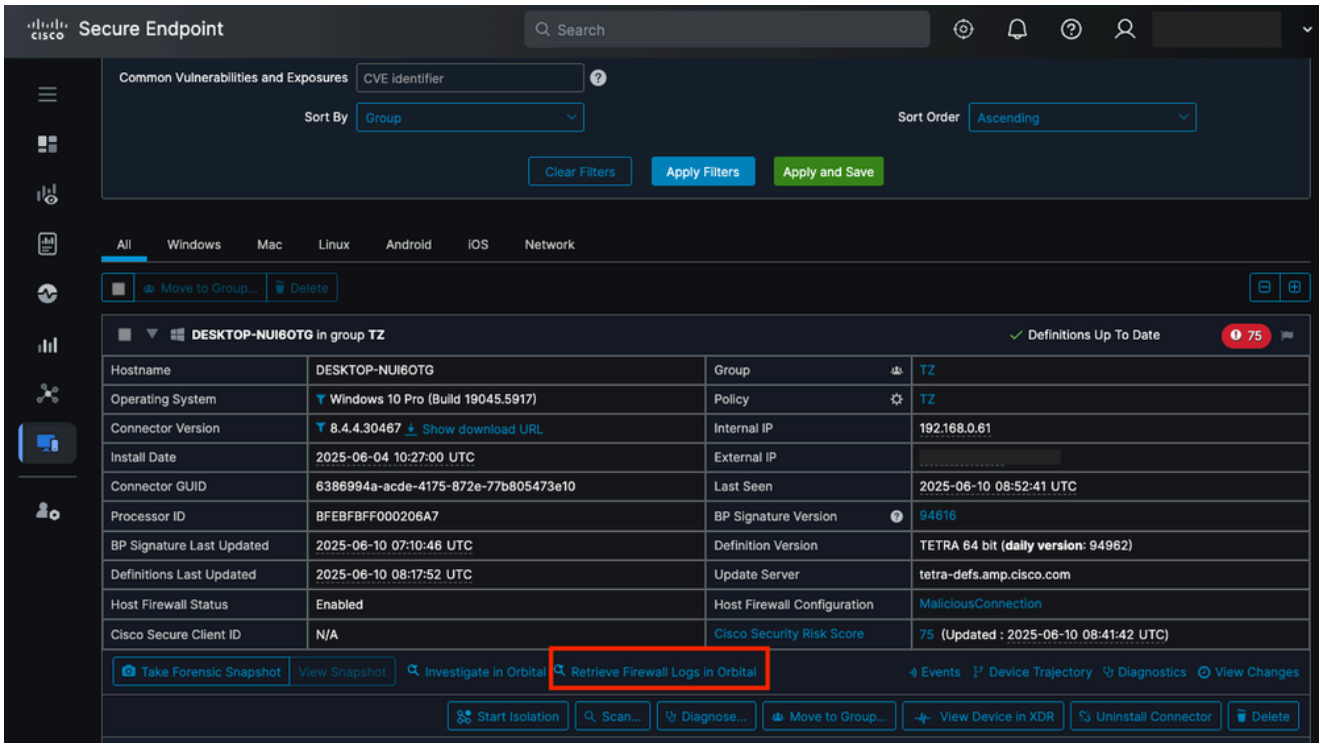
注意：日志文件位于<install directory>\Cisco\AMP\<Connector version>\FirewallLog.csv文件夹中

2.打开CSV文件以验证“阻止”操作规则的匹配项。使用过滤器区分“允许”和“阻止”连接。 

CSV文件中的防火墙日志

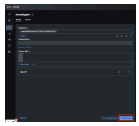
使用Orbital检索防火墙日志

1. 在安全终端门户中，导航到管理>计算机，找到终端，然后单击检索轨道中的防火墙日志。此操作会将您重定向到轨道门户。



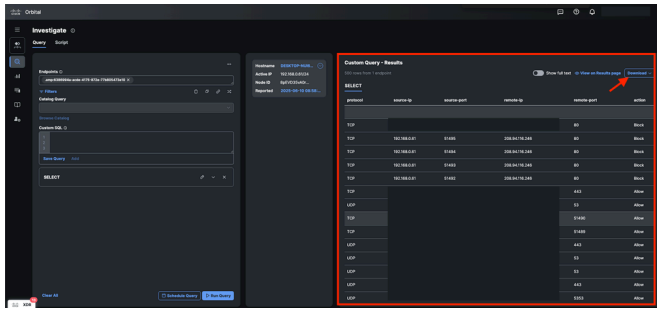
用于检索轨道中的防火墙日志的按钮

2. 在轨道门户中，点击运行查询。此操作显示在终端上记录的主机防火墙的所有日志。



从轨道运行查询

3. 信息显示在Resultstab中，或者您可以下载它。



轨道查询结果

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。