ホストファイアウォールによる悪意のある接続のトラブルシューティング

内容

はじめに

このドキュメントでは、Windowsエンドポイントで悪意のある接続を検出し、Cisco Secure Endpointのホストファイアウォールを使用してそれらをブロックする方法について説明します。

前提条件

要件

- ホストファイアウォールは、Secure Endpoint Advantageおよびプレミアパッケージで利用できます。
- サポートされるコネクタバージョン
  - Windows(x64):Secure Endpoint Windowsコネクタ8.4.2以降。
  - Windows(ARM):Secure Endpoint Windowsコネクタ8.4.4以降。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

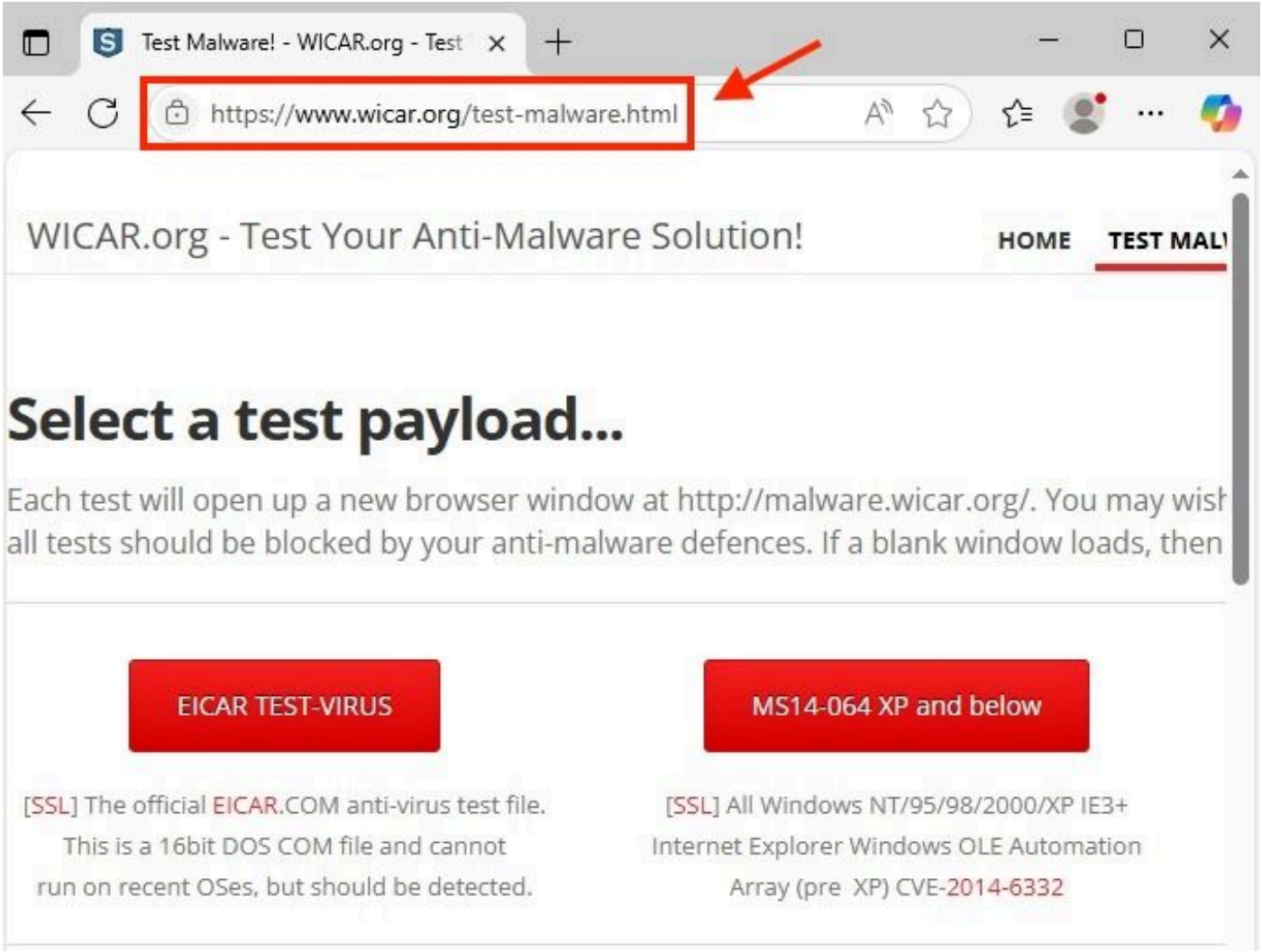
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トラブルシューティング ガイド

このドキュメントでは、Cisco Secure Endpoint Host Firewallを使用して悪意のある接続をブロックする方法について説明します。テストするには、テストページ malware.wicar.org(208.94.116.246)を使用して、トラブルシューティングガイドを作成します。

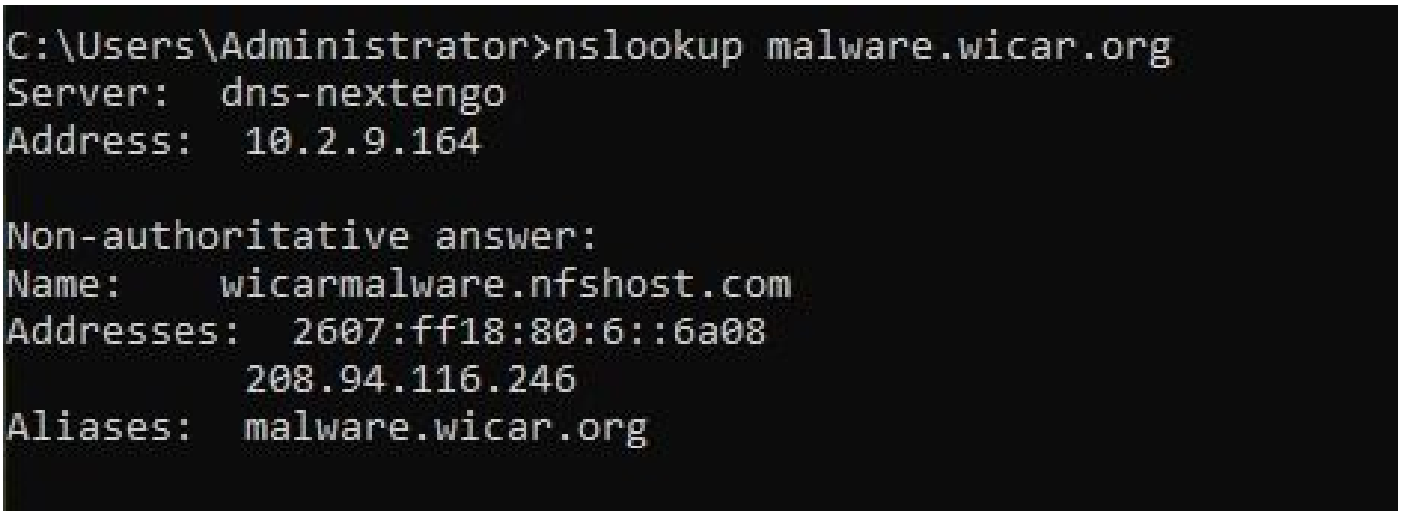
悪意のある接続を特定してブロックする手順

1. 最初に、確認してブロックするURLまたはIPアドレスを特定する必要があります。このシナリオでは、consider malware.wicar.orgです。
2. 次の図に示すように、URLへのアクセスがsuccessful. malware.wicar.orgで別のURLにリダイレクトされることを確認します。



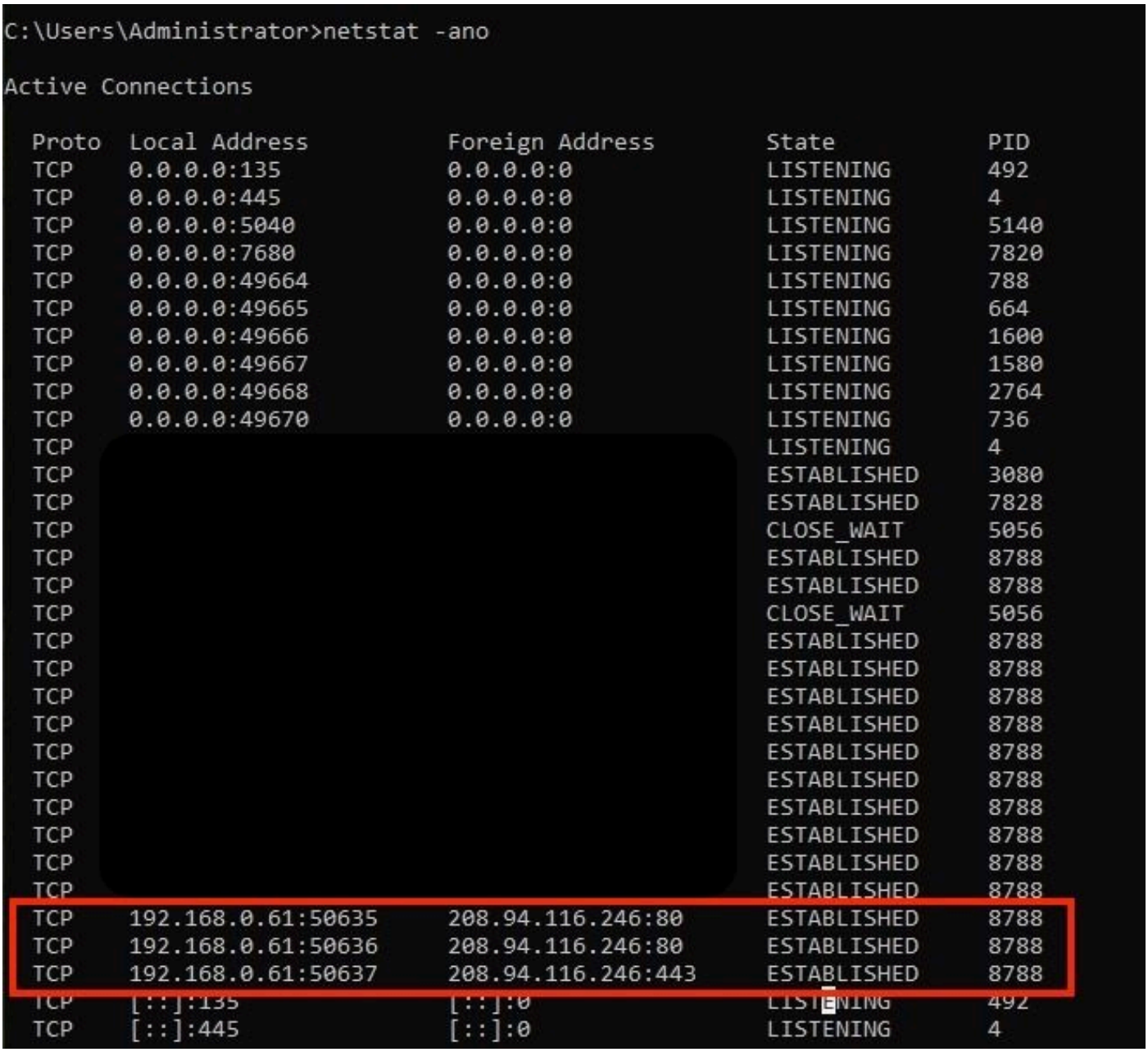
ブラウザの悪意のあるURL

3. nslookupコマンドを使用して、URL malware.wicar.orgに関連付けられたIPアドレスを取得します。



nslookupの出力

4. 悪意のあるIPアドレスを取得したら、コマンドnetstat -anoを使用してエンドポイントのアクティブな接続を確認します。



すべての接続のnetstat

5. アクティブな接続を切り離すには、フィルタを適用して、確立されている接続だけを表示します。

```
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>
```

確立された接続のnetstat

6.前の出力でthenslookupコマンドから取得したIPアドレスを探します。送信元IP、宛先IP、送信元ポート、および宛先ポートを特定します。

- ローカルIP:192.168.0.61
- リモートIP:208.94.116.246
- ローカルポート：該当なし
- 宛先ポート80および443

7. この情報を入手したら、Cisco Secure Endpoint Portalに移動し、ホストファイアウォール設定を作成します。

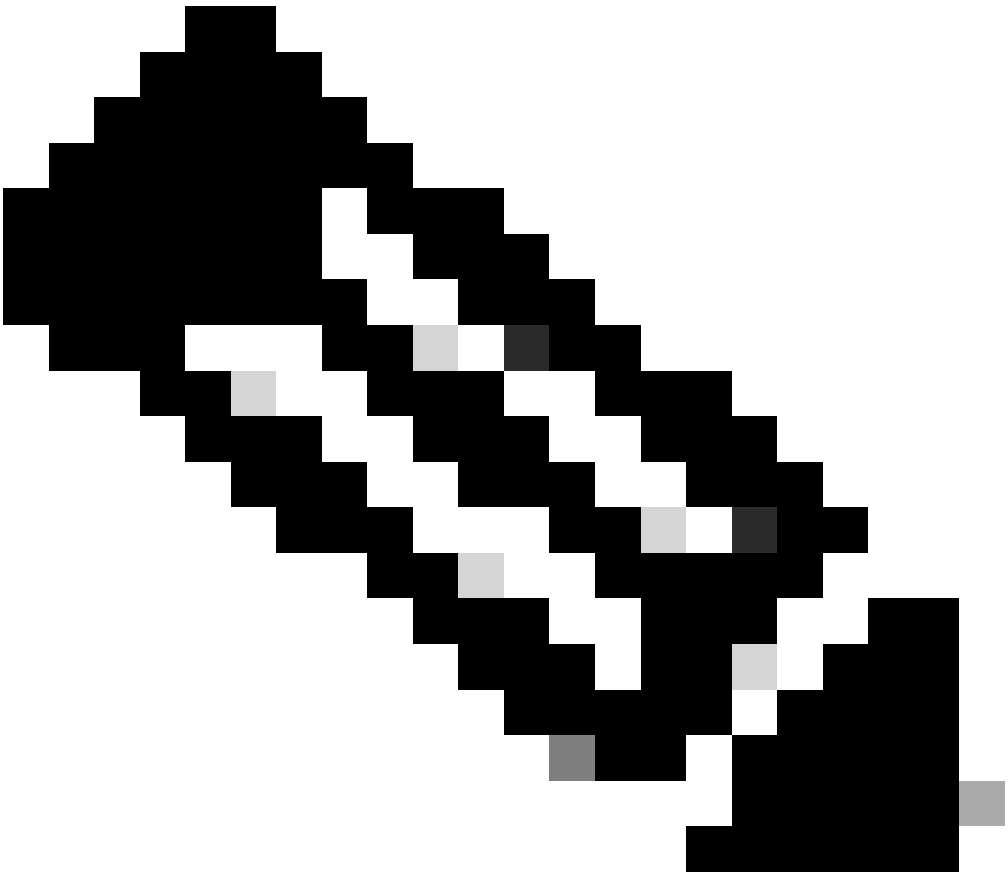
ホストファイアウォールの設定とルールの作成

1. Management > Host Firewallsの順に移動し、New Configurationをクリックします。 

   ホストファイアウォールの新しい設定

2. 名前を選択し、デフォルトアクションを選択します。この場合は、Allowを選択します。 

   ホストファイアウォールの設定名とデフォルトアクション

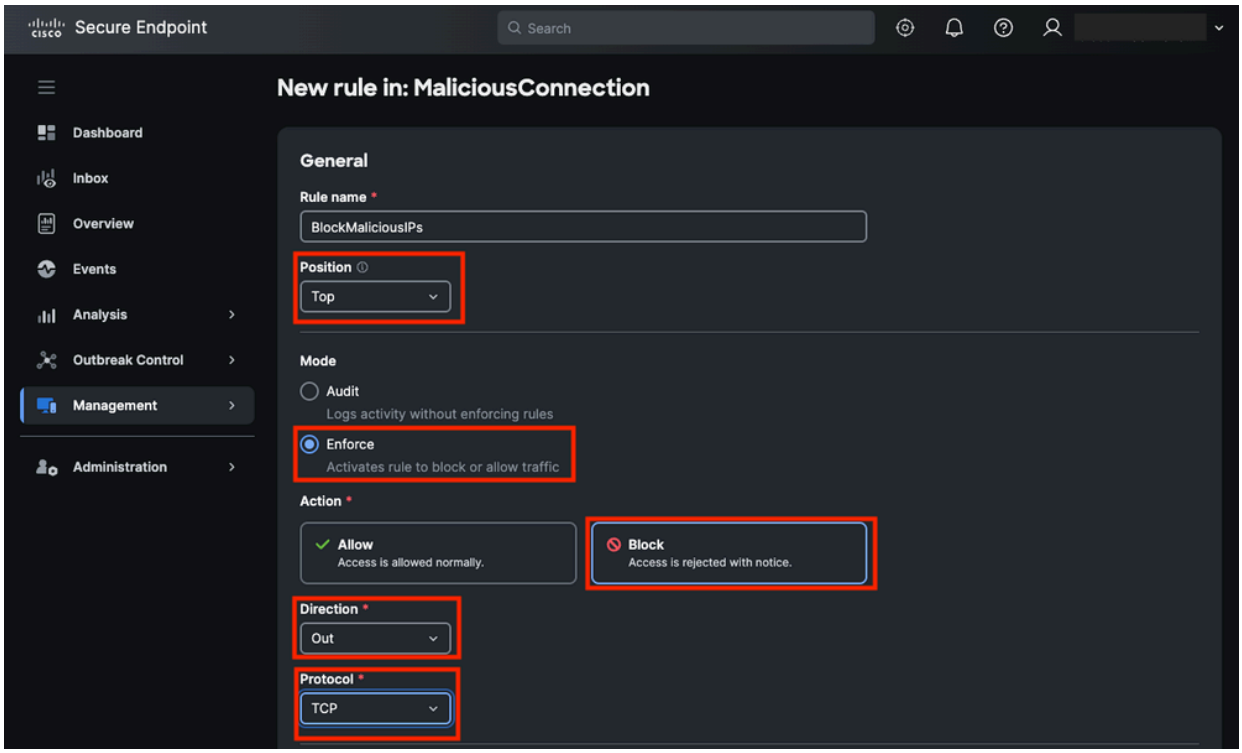


注：ブロックルールを作成しますが、正当な接続への影響を避けるために他のトラフィックを許可する必要があることに注意してください。

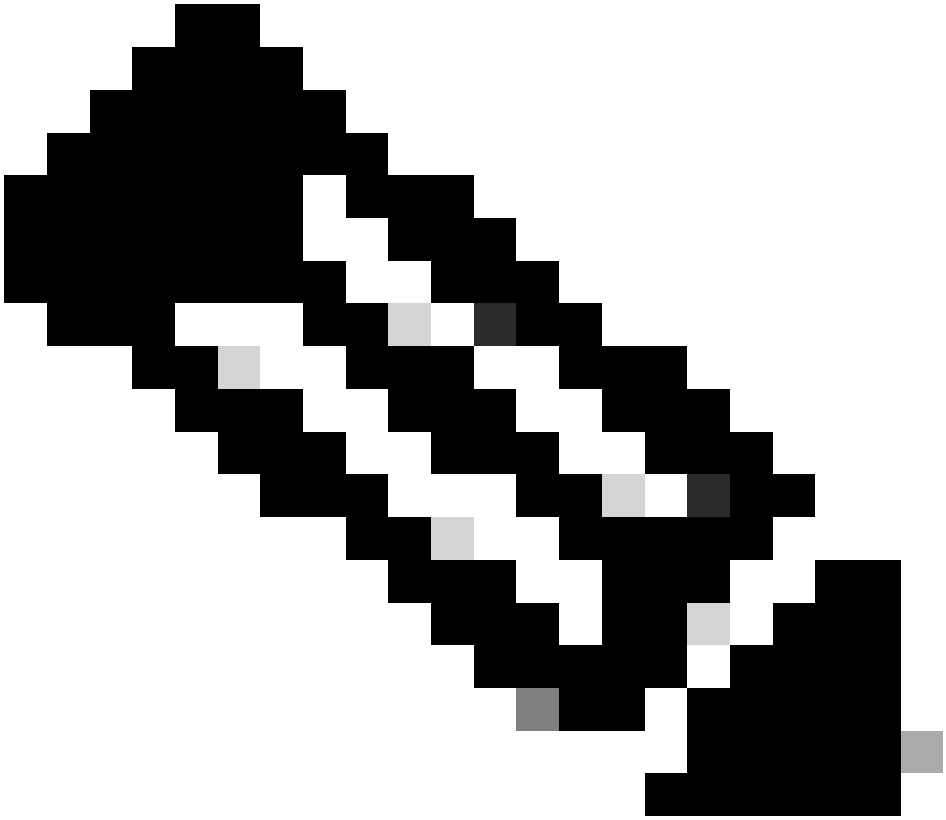
3. デフォルトルールが作成されたことを確認し、Add Ruleをクリックします。 

ホストファイアウォールに規則を追加

4. 名前を割り当て、次のパラメータを設定します。
   - 位置：上
   - モード：適用
   - アクション：ブロック
   - 方向：発信
   - プロトコル:TCP

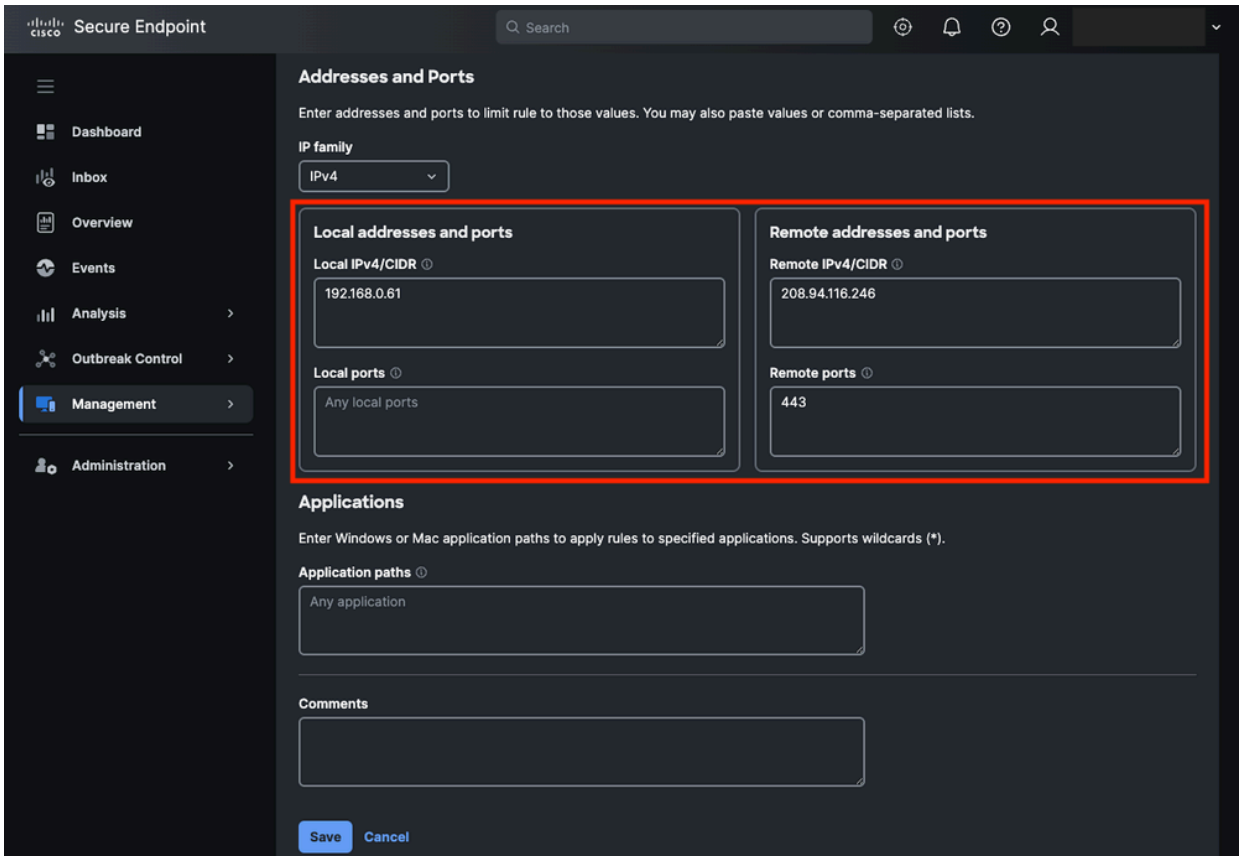


ルールの一般パラメータ



注：内部エンドポイントから外部の宛先（通常はインターネット）への悪意のある接続に対処する場合、方向は常にOutになる可能性があります。

5. ローカルIPと宛先IPを指定します。
   - ローカルIP:192.168.0.61
   - リモートIP:208.94.116.246
   - Localポートフィールドは空白のままにします。
   - 宛先ポートを80および443に設定します。これらはHTTPおよびHTTPSに対応します。

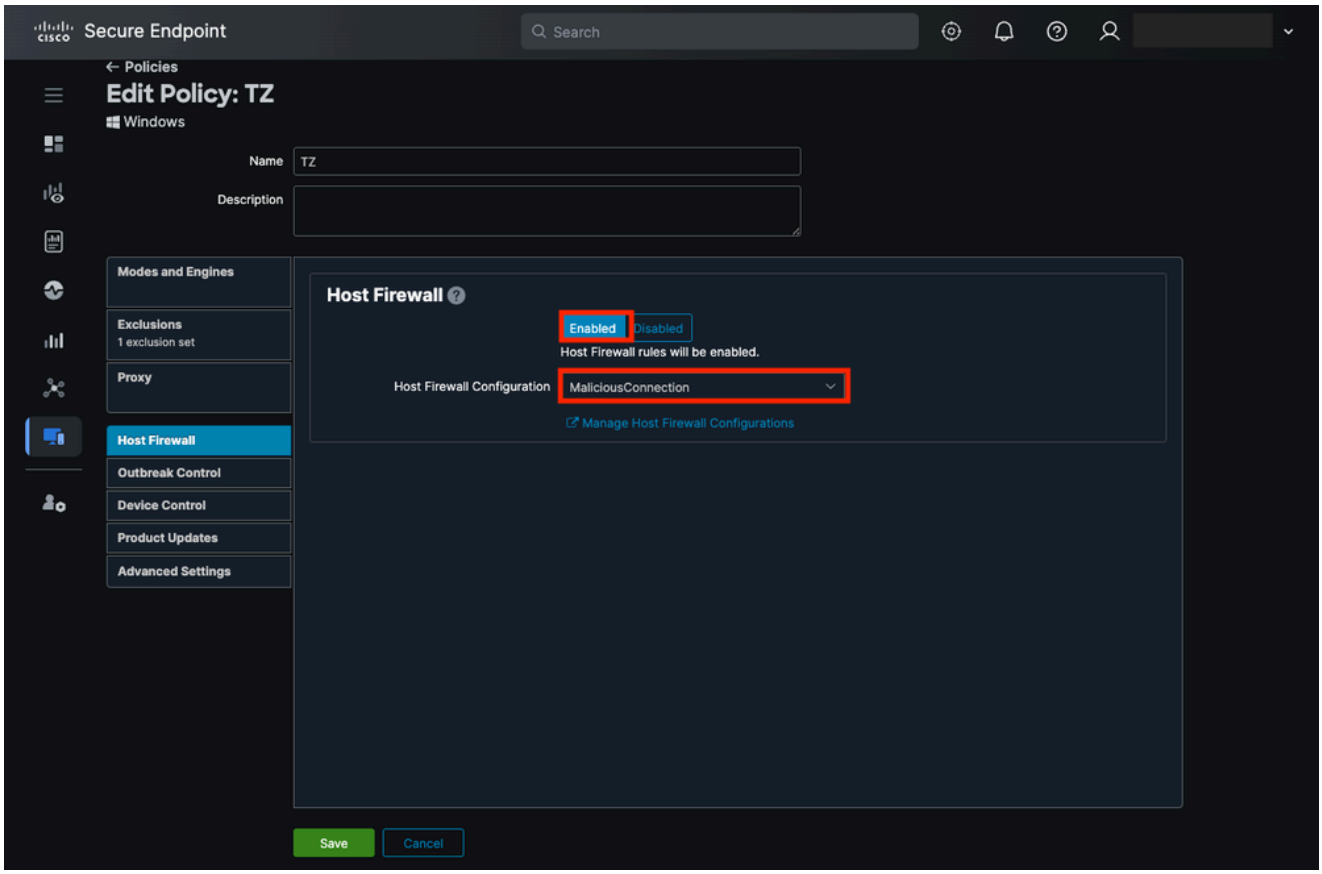


ルールのアドレスとポート

6. 最後に、Saveをクリックします。

ポリシーでホストファイアウォールを有効にし、新しい設定を割り当てる

1. Secure Endpoint Portalで、Management > Policiesの順に移動し、悪意のあるアクティビティをブロックするエンドポイントに関連付けられているポリシーを選択します。
2. Editorをクリックし、Host Firewallタブに移動します。
3. ホストファイアウォール機能を有効にして、最新の設定(この場合はMaliciousConnection)を選択します。



セキュアエンドポイントポリシーで有効にされたホストファイアウォール

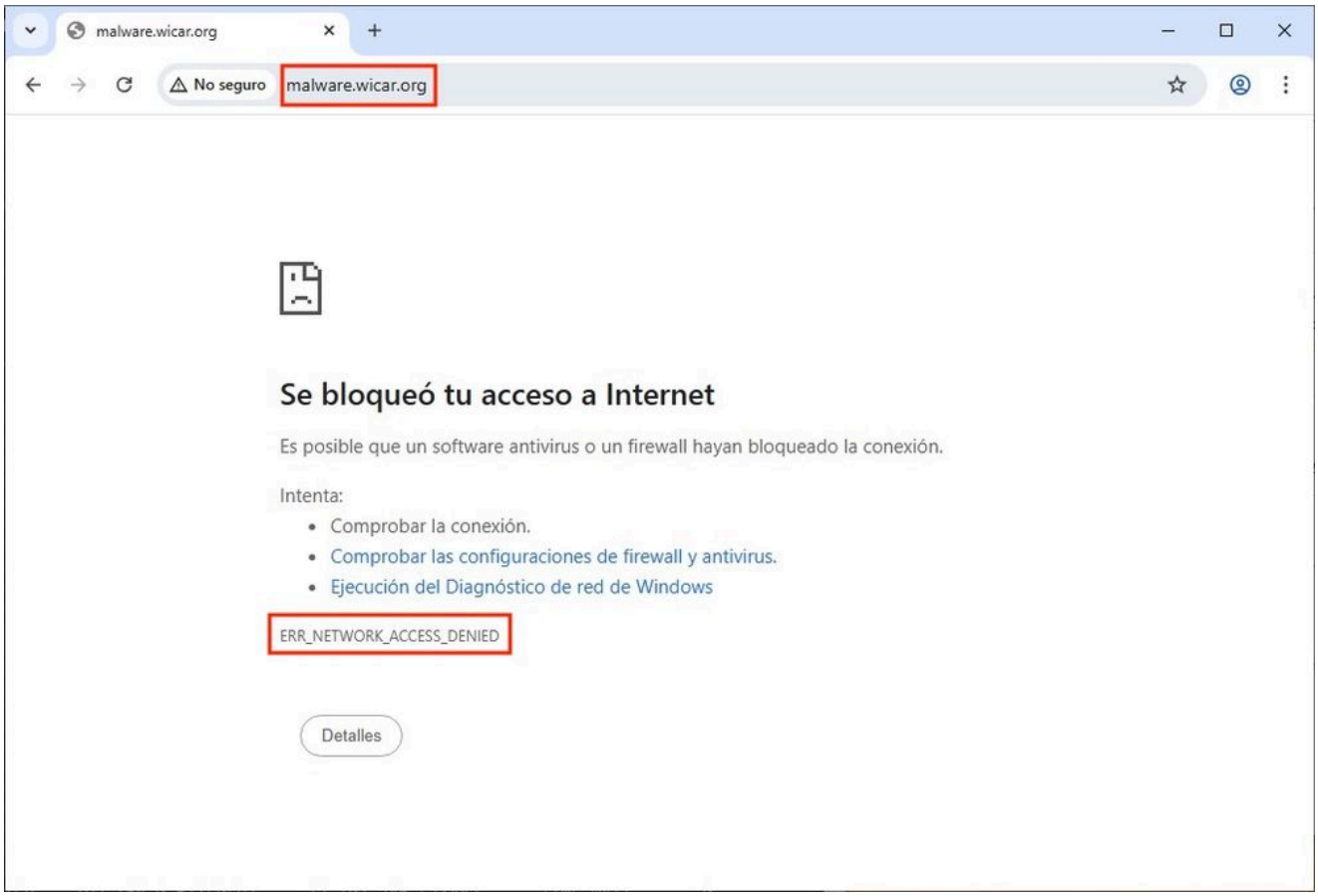
4. [Save] をクリックします。

5. 最後に、エンドポイントがポリシー変更を適用したことを確認します。 

ポリシー更新イベント

ローカルでの設定の検証

1. ブラウザでmalware.eicar.org というURLを使用して、ブロックされていることを確認します。



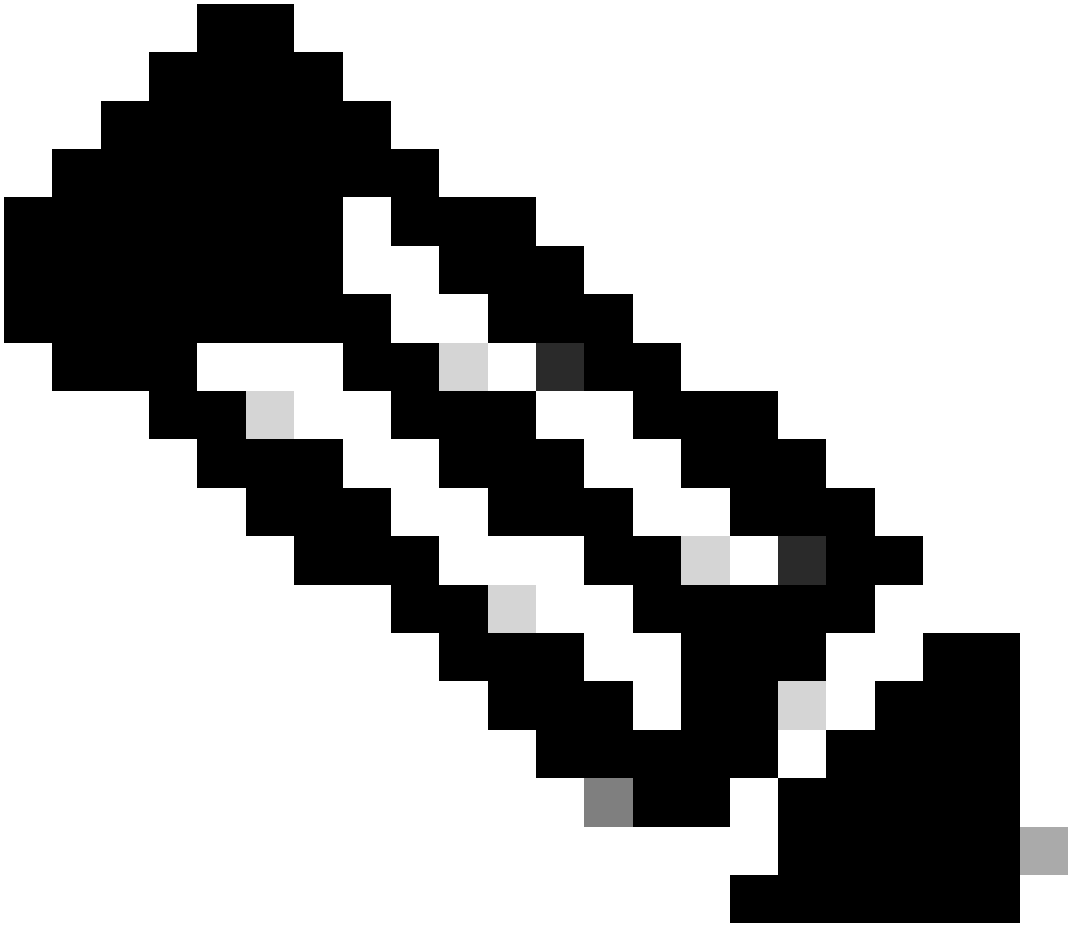
エラー「Network Access Denied from Browser」

2. ブロックを確認したら、接続が確立されていないことを確認します。netstat -ano | findstr ESTABLISHED コマンドを使用し、悪意のあるURL(208.94.116.246)に関連付けられているIPが表示されていないことを確認します。

ログの確認

1. エンドポイントで、フォルダに移動します。

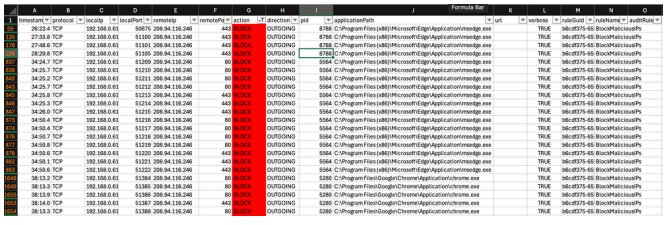
C:\Program Files\Cisco\AMP\<コネクタバージョン>\FirewallLog.csv



注：ログファイルは、<install directory>\Cisco\AMP\<Connector version>\FirewallLog.csvフォルダにあります

---

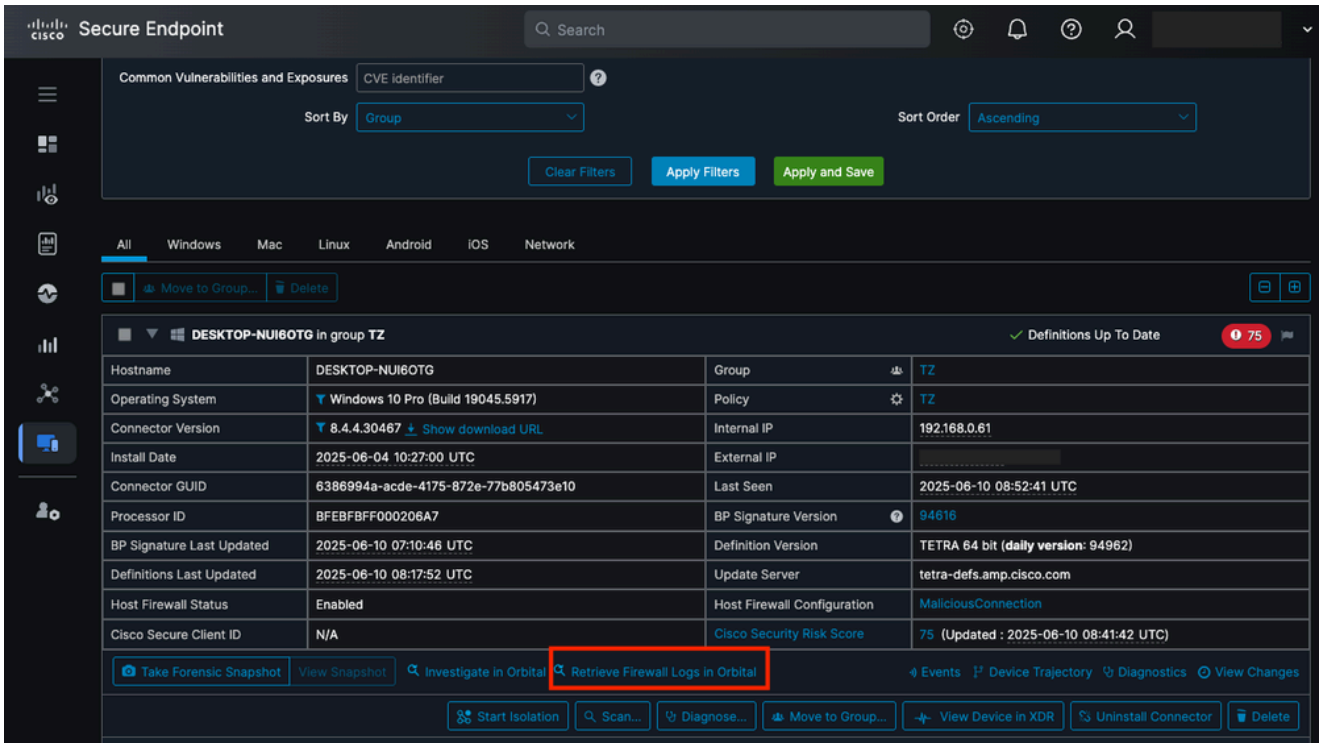
2. CSVファイルを開いて、ブロックアクションルールの一致を検証します。フィルタを使用して、許可する接続とブロックする接続を区別します。



CSVファイルのファイアウォールログ

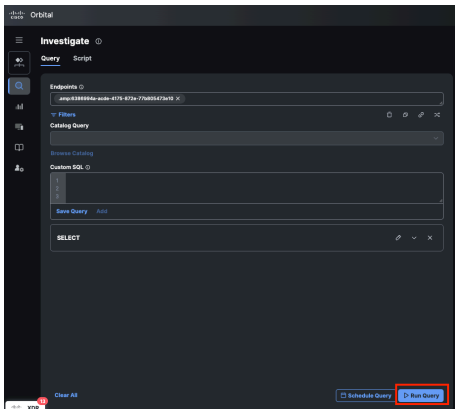
Orbitalを使用したファイアウォールログの取得

1. Secure Endpoint Portalで、Management > Computersの順に移動し、エンドポイントを見つけて、Retrieve Firewall Logs in Orbitalをクリックします。この操作により、Orbital Portalにリダイレクトされます。



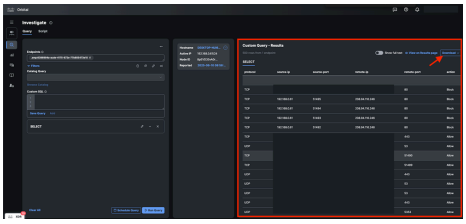
Orbitalでファイアウォールログを取得するボタン

2. Orbital PortalでRun Queryをクリックします。このアクションは、ホストファイアウォール



のエンドポイントで記録されたすべてのログを表示します。

オービタルからクエリを実行



3. 情報はResultstabに表示されるか、ダウンロードできます。

オービタルからのクエリ結果

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。