Solucionar problemas de conexão mal-intencionada com o firewall do host

Contents

Introdução

Este documento descreve como detectar conexões mal-intencionadas em um endpoint do Windows e bloqueá-las usando o Host Firewall no Cisco Secure Endpoint.

Pré-requisitos

Requisitos

- O Host Firewall está disponível com os pacotes Secure Endpoint Advantage e Premier.
- Versões de Conector Suportadas
  - Janelas (x64): Conector Secure Endpoint para Windows 8.4.2 e posterior.
  - Janelas (ARM): Conector Secure Endpoint para Windows 8.4.4 e posterior.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

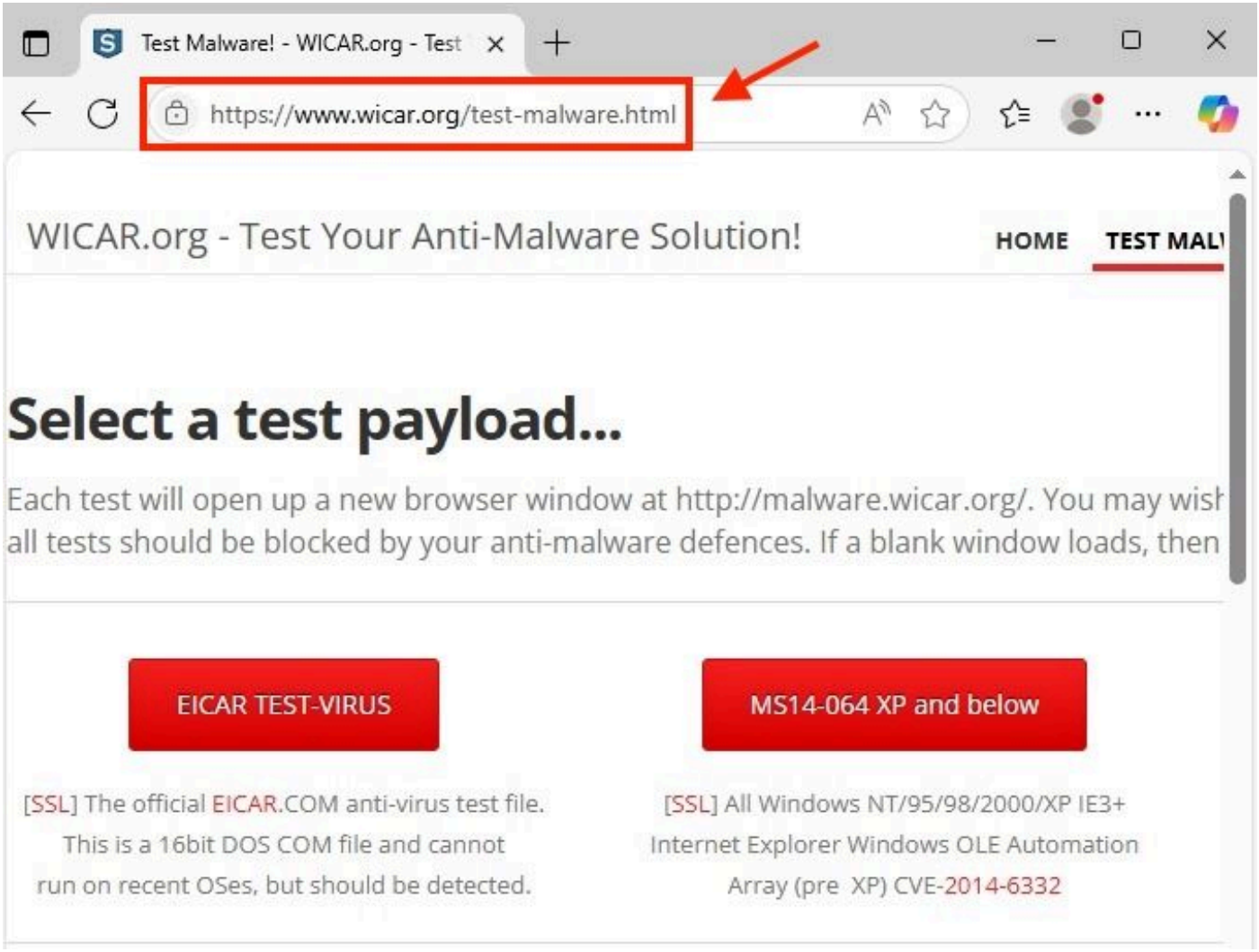
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Guia de solução de problemas

Este documento fornece um guia para bloquear conexões mal-intencionadas com o uso do Cisco Secure Endpoint Host Firewall. Para testar, use a página de teste malware.wicar.org (208.94.116.246) para criar um guia de solução de problemas.

Etapas para identificar e bloquear conexões mal-intencionadas

1. Primeiro, você precisa identificar o URL ou o endereço IP que deseja revisar e bloquear. Para este cenário, consider malware.wicar.org.
2. Verifique se o acesso à URL é successful. malware.wicar.org redireciona para uma URL diferente, como mostrado na imagem.



URL mal-intencionada do navegador

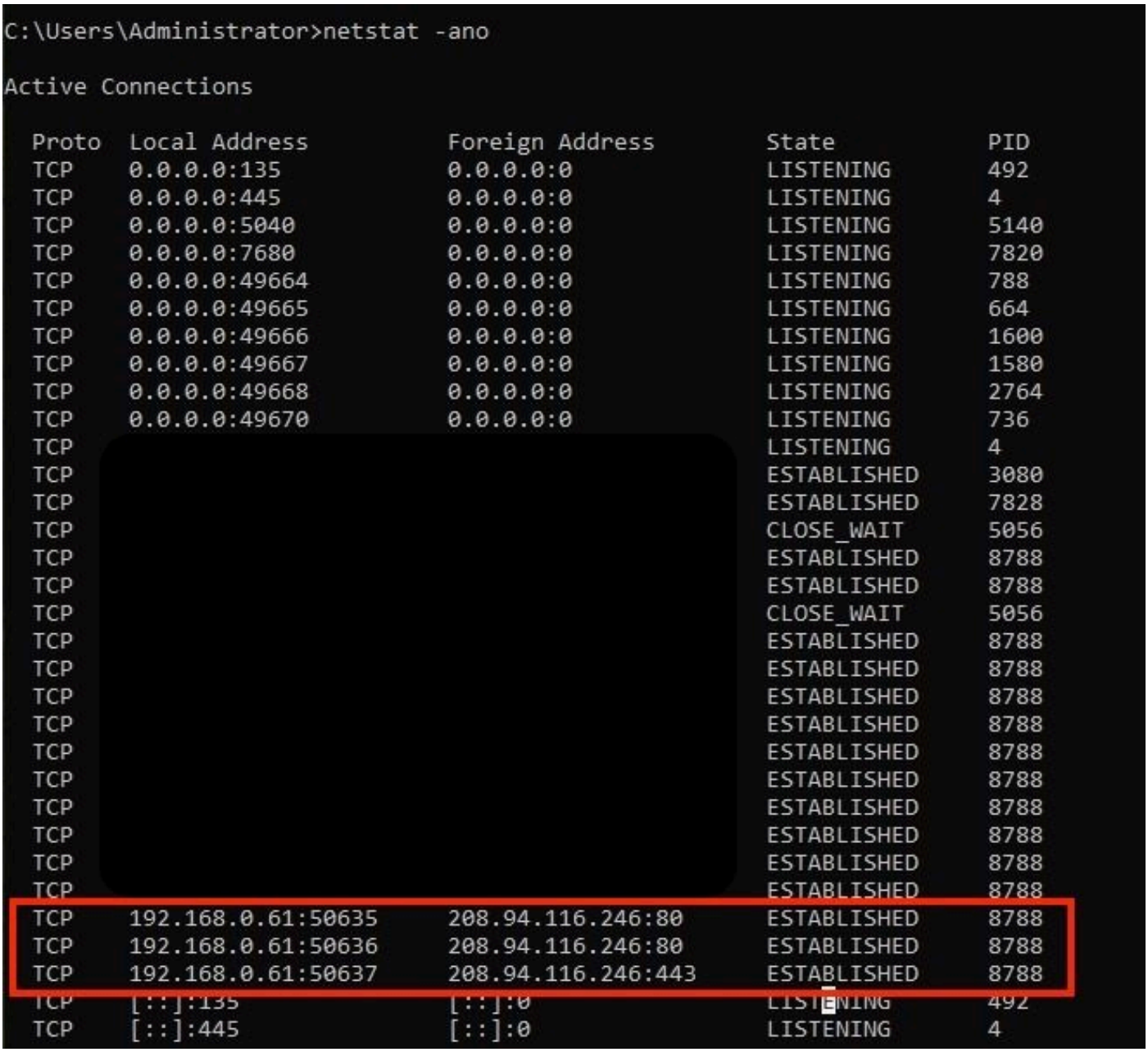
3. Use o comando nslookup para recuperar o endereço IP associado à URL malware.wicar.org.

```
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
```

Saída de nslookup

4. Uma vez obtido o endereço IP mal-intencionado, verifique as conexões ativas no endpoint com o comando:netstat -ano.



netstat para todas as conexões

5. Para isolar conexões ativas, aplique um filtro para exibir apenas conexões estabelecidas.

```
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>
```

netstat para conexões estabelecidas

6. Procure o endereço IP obtido do comando enslookup na saída anterior. Identifique o IP origem, o IP destino, a porta origem e a porta destino.

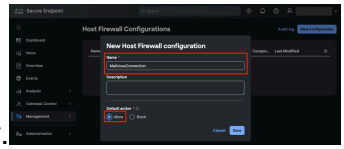
- IP local: 192.168.0.61
- IP remoto: 208.94.116.246
- Porta local: Não aplicável
- Porta de destino para 80 e 443

7. Depois de obter essas informações, navegue até o Cisco Secure Endpoint Portal para criar a configuração do Host Firewall.

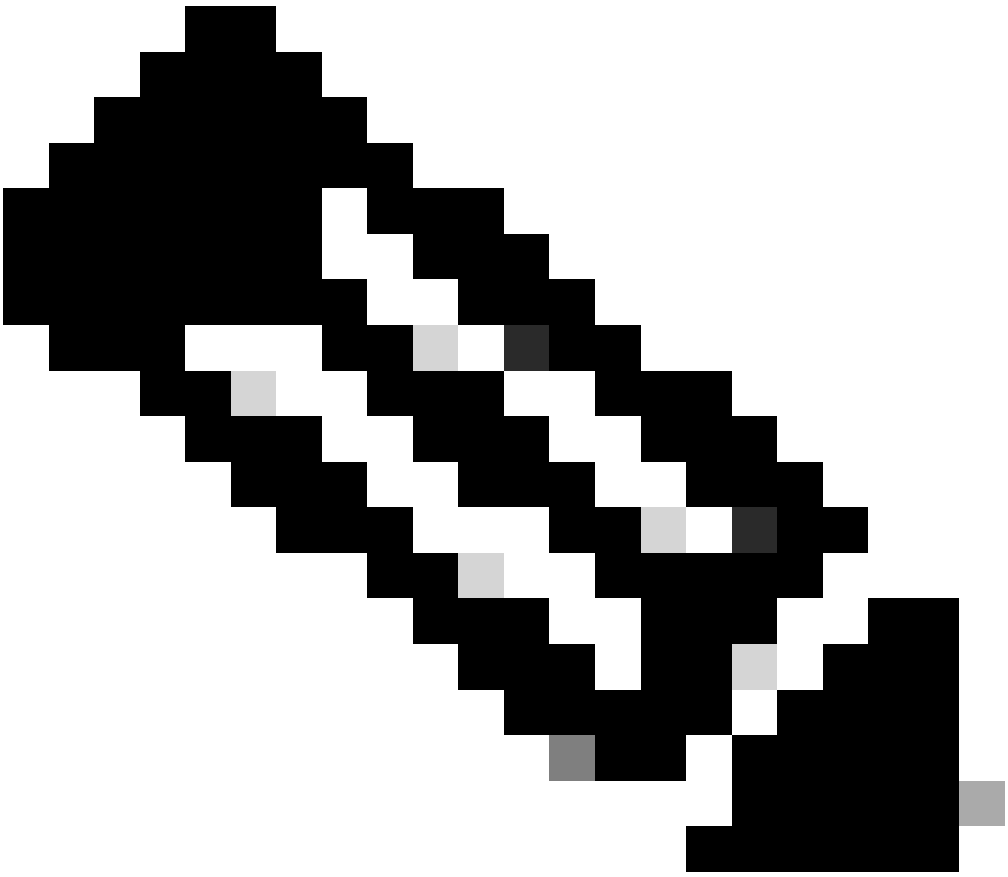
Configuração do firewall do host e criação de regras

1. Navegue paraGerenciamento > Firewall do host e clique emNova configuração. 

   Nova configuração do firewall do host

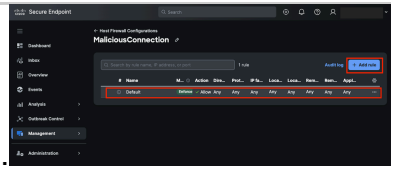
2. Selecione um nome e aAção padrão. Nesse caso, selecione Permitir. 

   Nome da Configuração do Firewall do Host e Ação Padrão



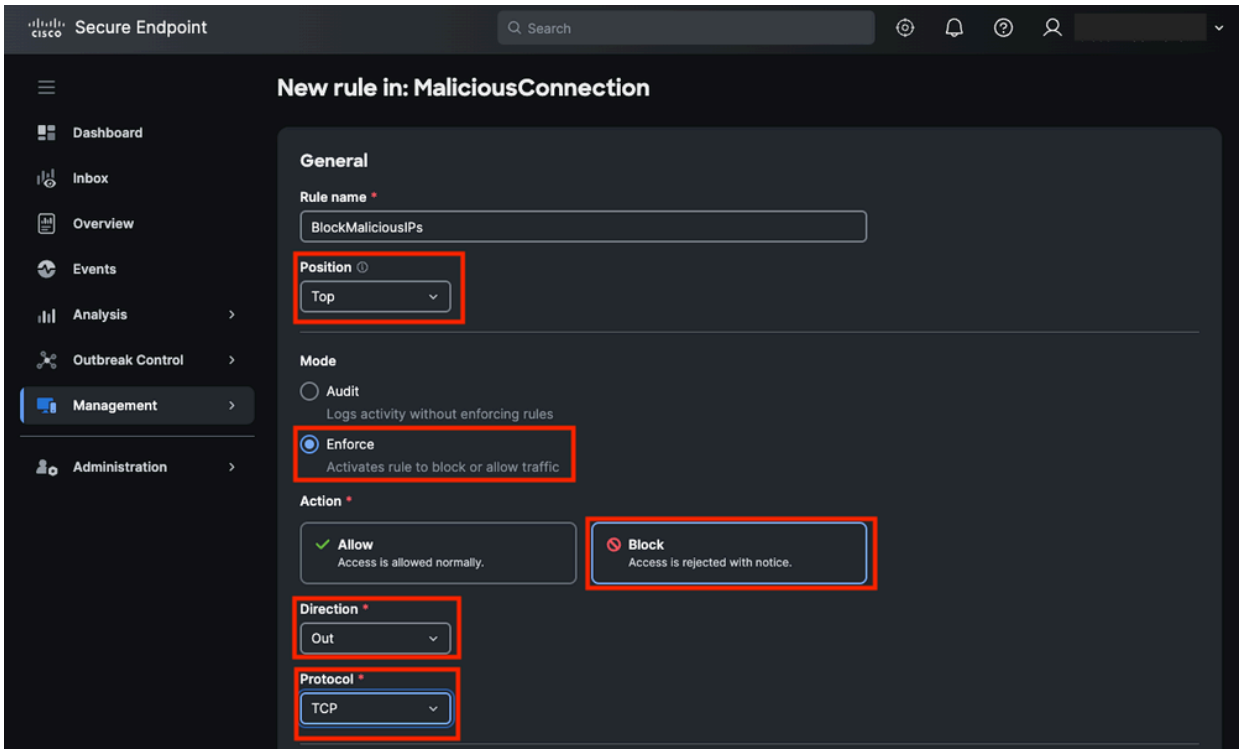
Note: Lembre-se de que você cria uma regra de bloqueio, mas deve permitir que outros tráfegos evitem impactos em conexões legítimas.

3. Verifique se a regra padrão foi criada e clique em Adicionar regra.

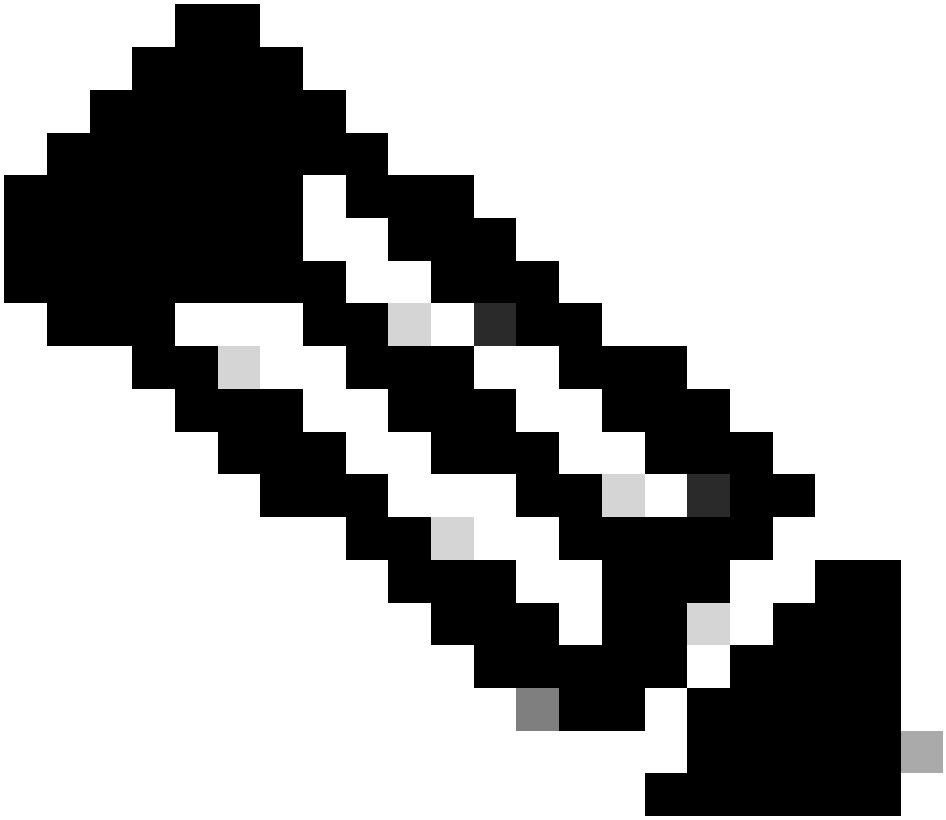


Adicionar regra no firewall do host

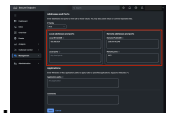
4. Atribua um nome e defina os próximos parâmetros:
    - Posição: Superior
    - Modo: Aplicar
    - Ação: Bloqueio
    - Direção: OUT
    - Protocolo: TCP



Parâmetros Gerais da Regra



Note: Quando você endereça conexões mal-intencionadas de um endpoint interno para um destino externo, geralmente para a Internet, a direção pode ser sempre Out.

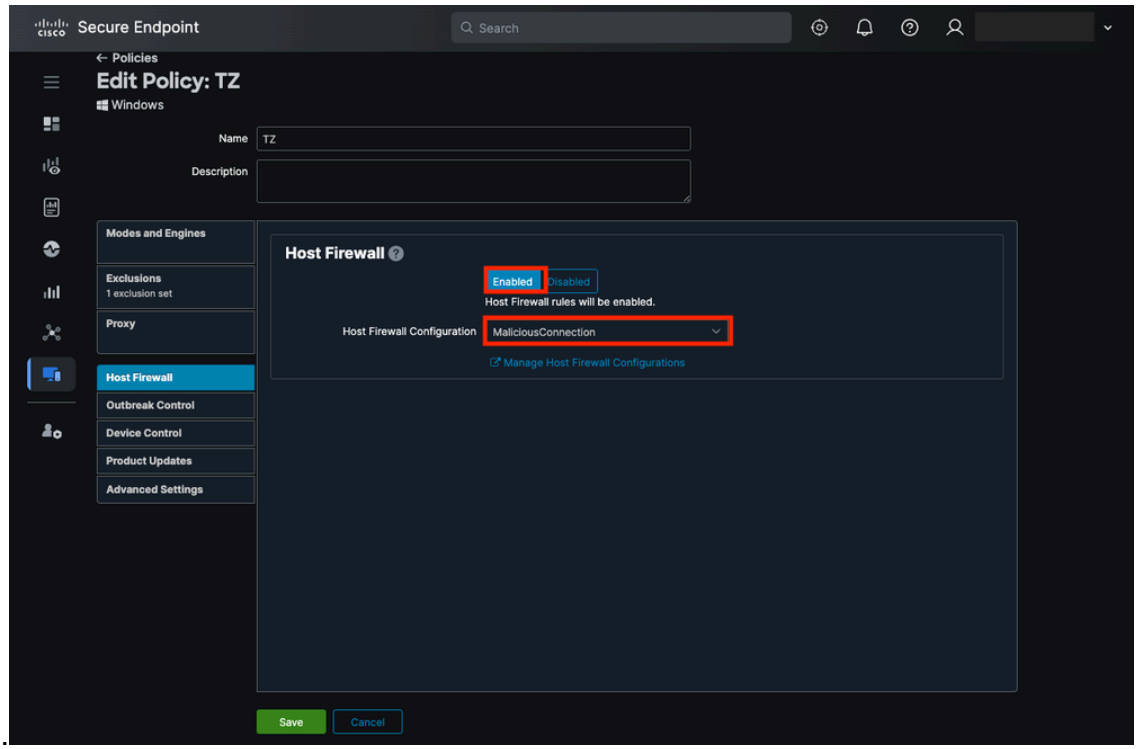
5. Especifique os IPs local e destino:
    - IP local: 192.168.0.61
    - IP remoto: 208.94.116.246
    - Deixe o campo Local em branco.
    - Defina Destination Portpara 80 e 443, que correspondem a HTTP e HTTPS. 

      Endereços e Portas de Regra

6. Finalmente, clique emSalvar.

Ative o firewall do host na política e atribua a nova configuração

1. No Secure Endpoint Portal, navegue paraManagement > Policies e selecione a política associada ao endpoint onde você deseja bloquear atividades mal-intencionadas.
2. Clique em Editar e navegue até a guia Firewall do Host.
3. Ative o recurso Host Firewall e selecione a configuração recente, neste caso Conexão mal-

intencionada. 

Firewall do Host Habilitado na Política de Ponto de Extremidade Seguro

4. Click Save.

5. Finalmente, verifique se o ponto final aplicou as alterações de política. 

Evento de Atualização de Política

Validar a configuração localmente

1. Use o URL malware.eicar.org em um navegador para confirmar que ele está bloqueado. 

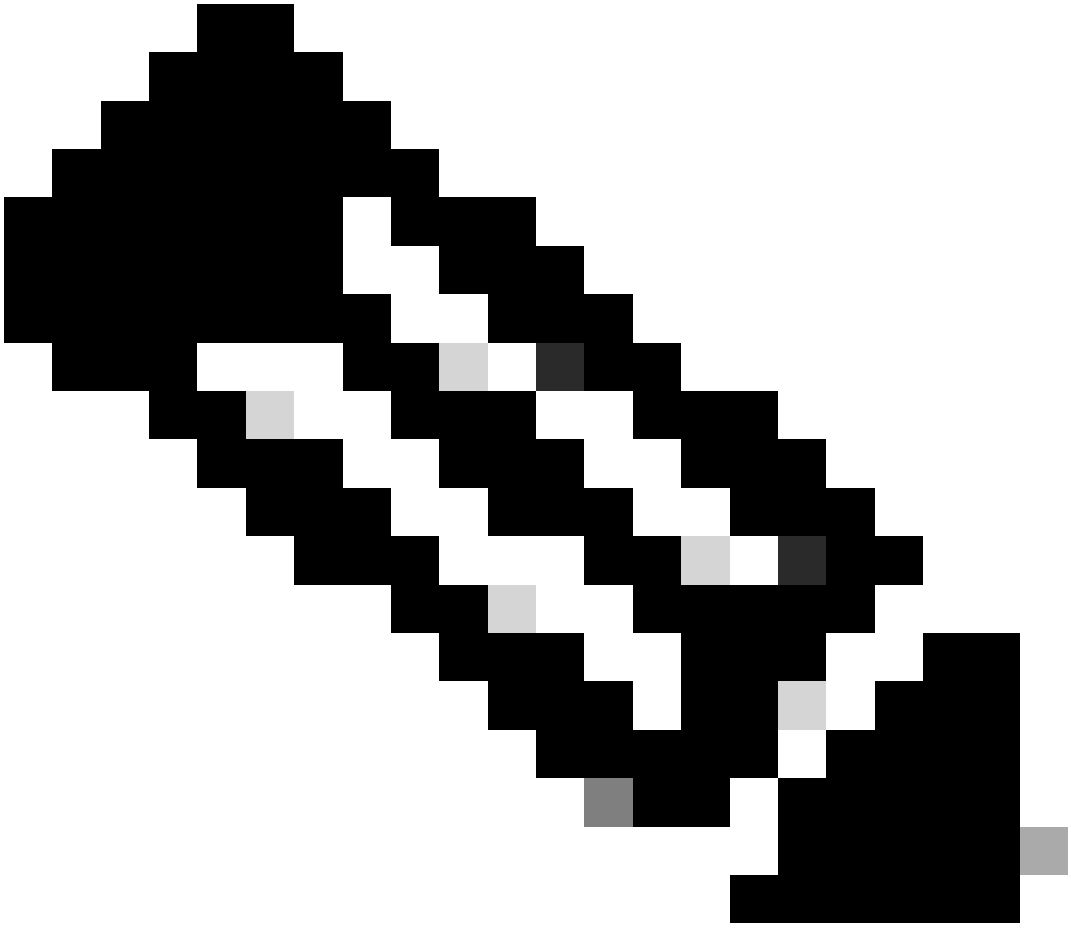
Erro Acesso à Rede Negado pelo Navegador

2. Depois de confirmar o bloqueio, verifique se não há conexões estabelecidas. Use o comando netstat -ano | findstr ESTABLISHED para garantir que o IP associado ao URL mal-intencionado (208.94.116.246) não esteja visível.

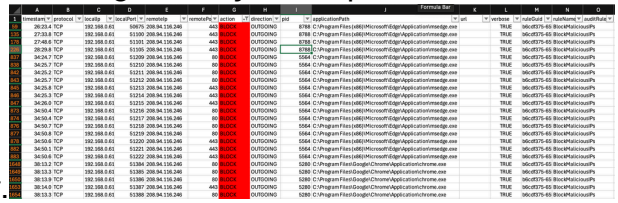
Logs de revisão

1. No endpoint, navegue até a pasta:

C:\Program Files\Cisco\AMP\<Connector version>\FirewallLog.csv



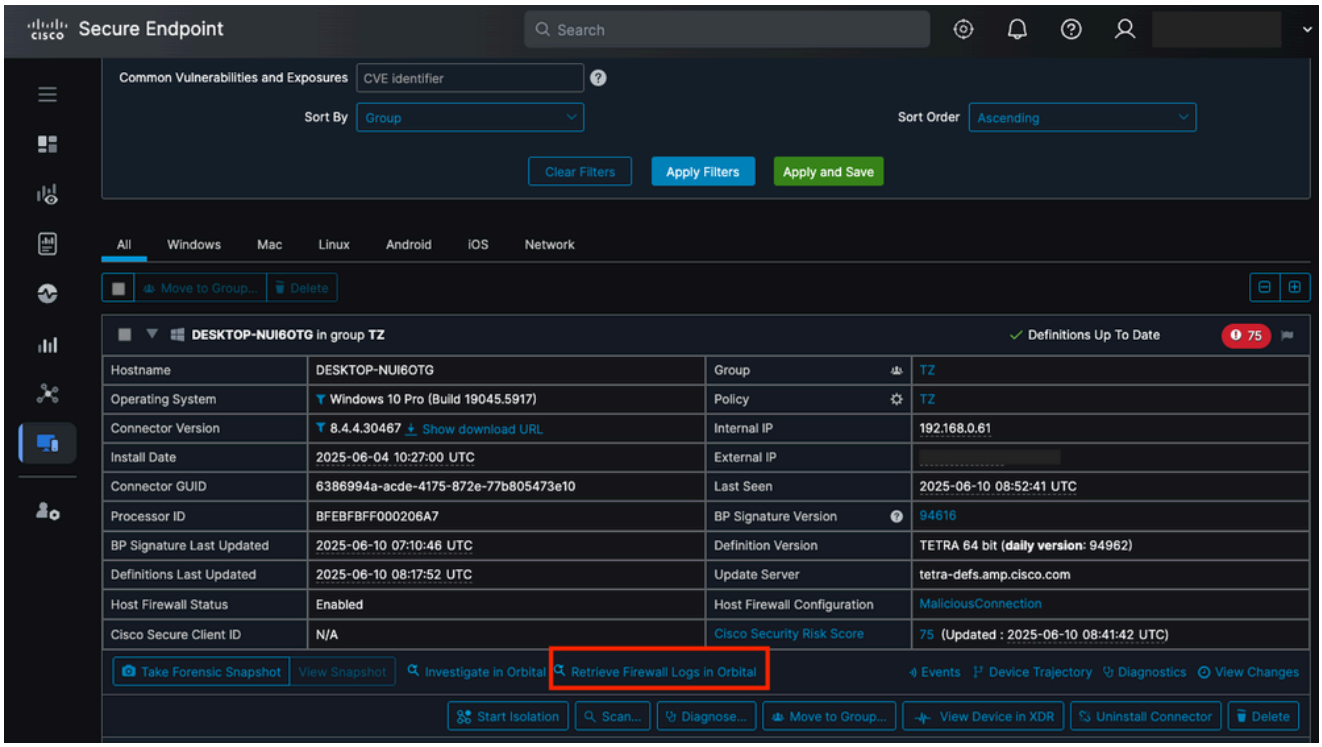
Note: O arquivo de log está localizado na pasta <diretório de instalação>\Cisco\AMP\<versão do Conector>\FirewallLog.csv

2. Abra o arquivo CSV para validar correspondências para a regra de ação Bloquear. Use um filtro para distinguir entre conexões Permitir e Bloquear. 

Logs de firewall no arquivo CSV

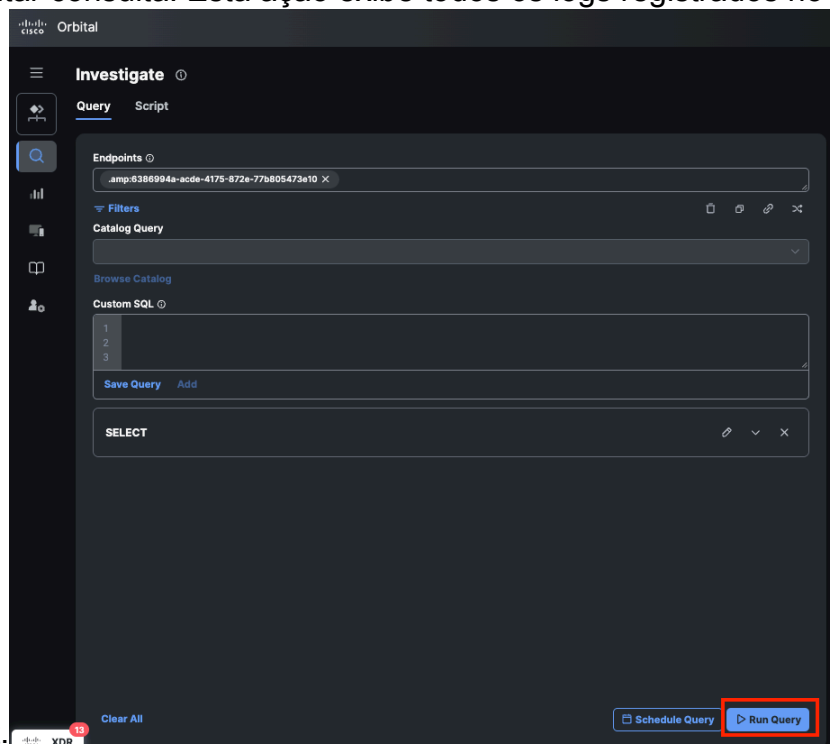
Usar Orbital para recuperar logs de firewall

1. No Secure Endpoint Portal, navegue paraGerenciamento > Computadores, localize o endpoint e clique em Recuperar logs de firewall no Orbital. Esta ação o redireciona para o Portal Orbital.



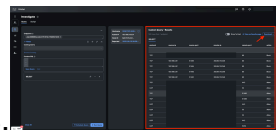
Botão para recuperar logs de firewall no Orbital

2. No Portal Orbital, clique em Executar consulta. Esta ação exibe todos os logs registrados no ponto final para o Firewall do Host.



Executar consulta a partir do Orbital

3. As informações ficam visíveis na guia Resultados ou você pode baixá-las.



Resultados da Consulta de Orbital

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.