Solución de problemas de conexión maliciosa con firewall de host

Contenido

Introducción

Este documento describe cómo detectar conexiones maliciosas en un terminal de Windows y bloquearlas usando el Firewall de host en el terminal seguro de Cisco.

Prerequisites

Requirements

- Host Firewall está disponible con los paquetes Secure Endpoint Advantage y Premier.
- Versiones de conector compatibles
  - Windows (x64): Conector Secure Endpoint Windows 8.4.2 y versiones posteriores.
  - Ventanas (ARM): Conector Secure Endpoint para Windows 8.4.4 y versiones posteriores.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

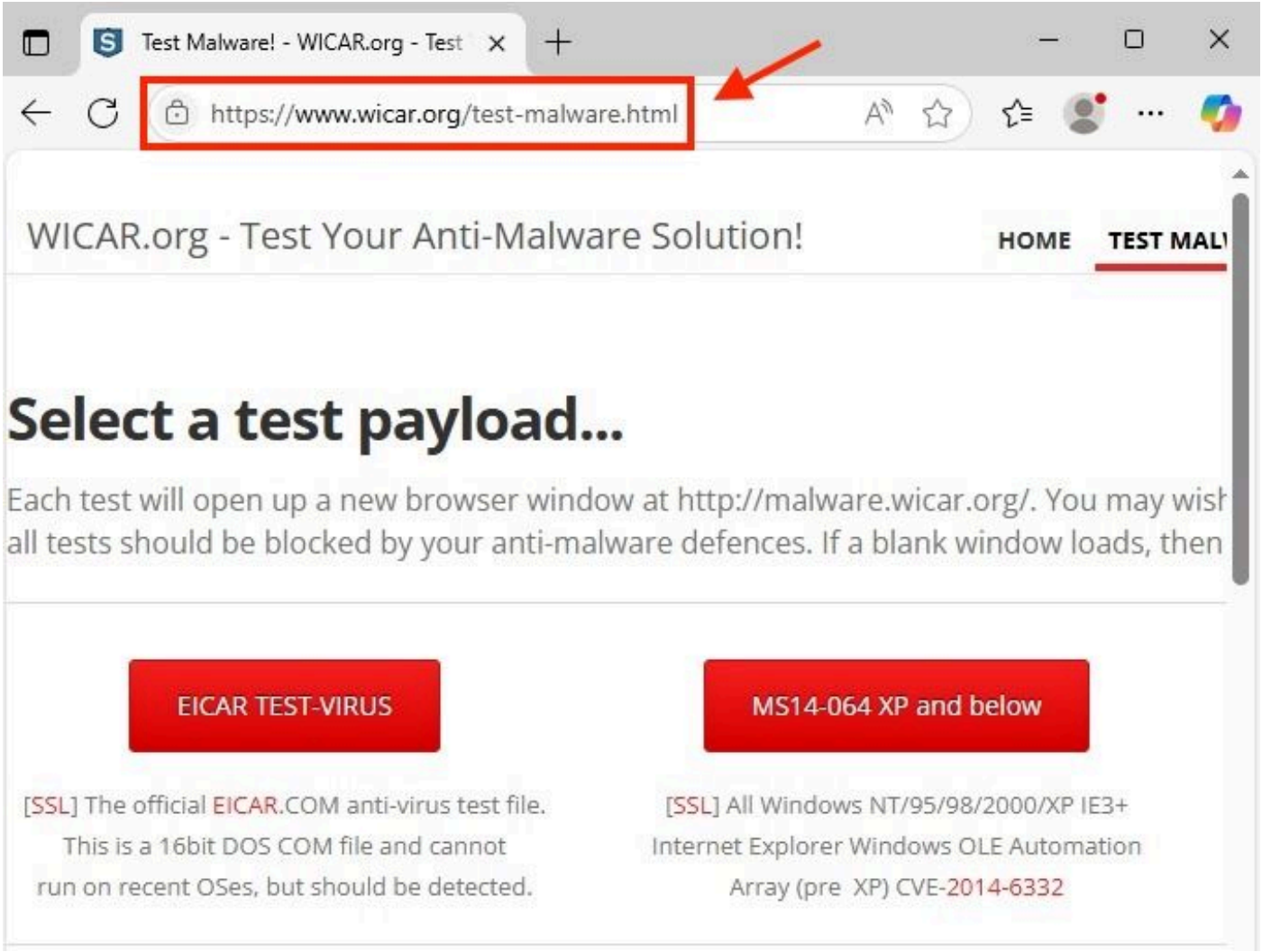
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Guía de Troubleshooting

Este documento proporciona una guía para bloquear conexiones maliciosas con el uso de Cisco Secure Endpoint Host Firewall. Para realizar la prueba, utilice la página de prueba malware.wicar.org (208.94.116.246) para crear una guía de solución de problemas.

Pasos para identificar y bloquear conexiones maliciosas

1. En primer lugar, debe identificar la URL o la dirección IP que desea revisar y bloquear. Para este escenario, consider malware.wicar.org.
2. Verifique si el acceso a la URL es successful. malware.wicar.org redirecciona a una URL diferente, como se muestra en la imagen.



URL maliciosa del navegador

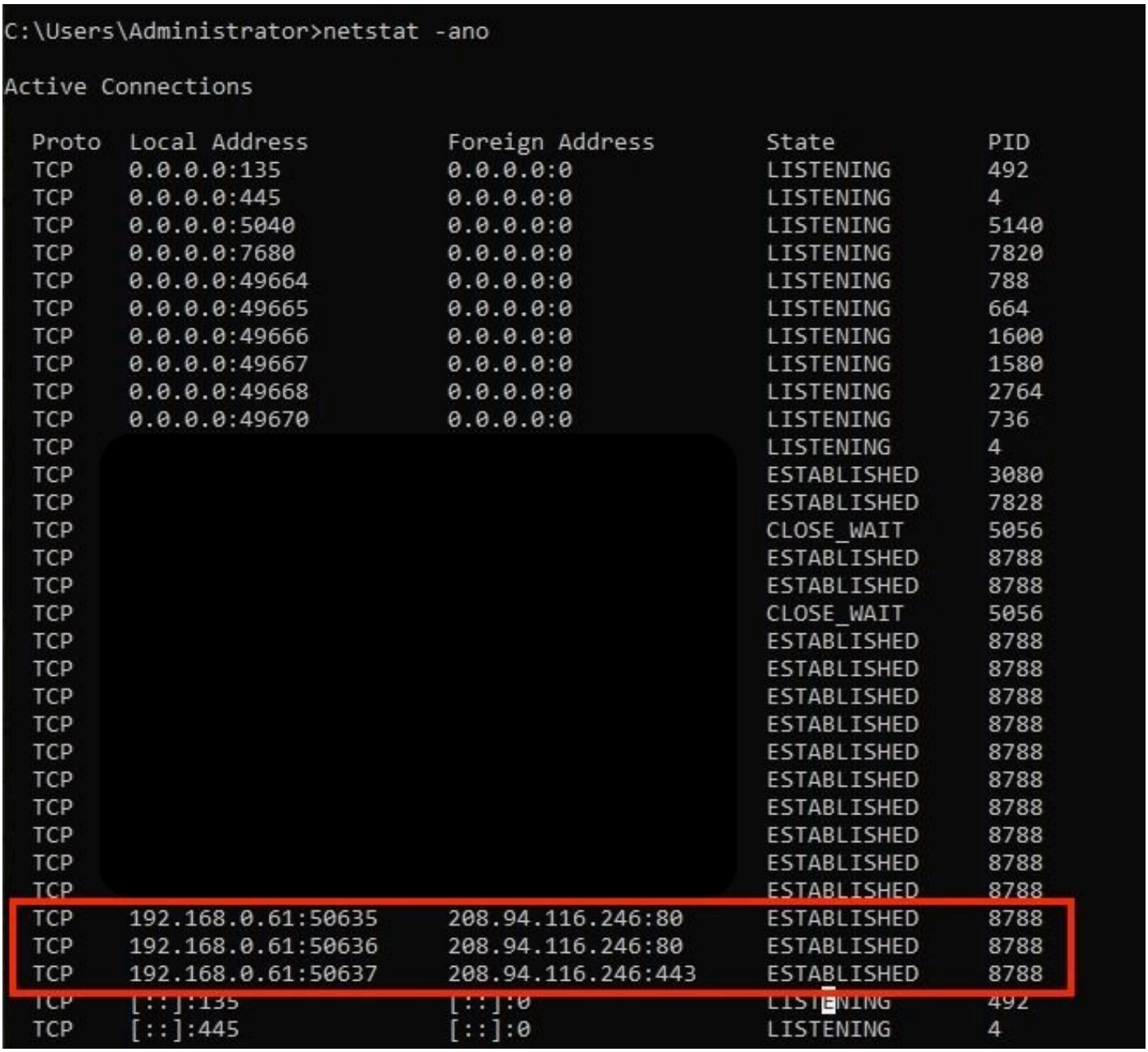
3. Utilice el comando nslookup para recuperar la dirección IP asociada a la dirección URL malware.wicar.org.

```
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
```

Resultado de nslookup

4. Una vez obtenida la dirección IP maliciosa, verifique las conexiones activas en el terminal con el comando:netstat -ano.



netstat para todas las conexiones

5. Para aislar las conexiones activas, aplique un filtro para mostrar solamente las conexiones establecidas.

```
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 conexiones establecidas

6. Busque la dirección IP obtenida del comando slookup en el resultado anterior. Identifique la IP de origen, la IP de destino, el puerto de origen y el puerto de destino.

- IP local: 192.168.0.61
- IP remota: 208.94.116.246
- Puerto local: No aplicable
- Puerto de destino 80 y 443

7. Una vez que disponga de esta información, navegue hasta Cisco Secure Endpoint Portal para crear la configuración de Host Firewall.

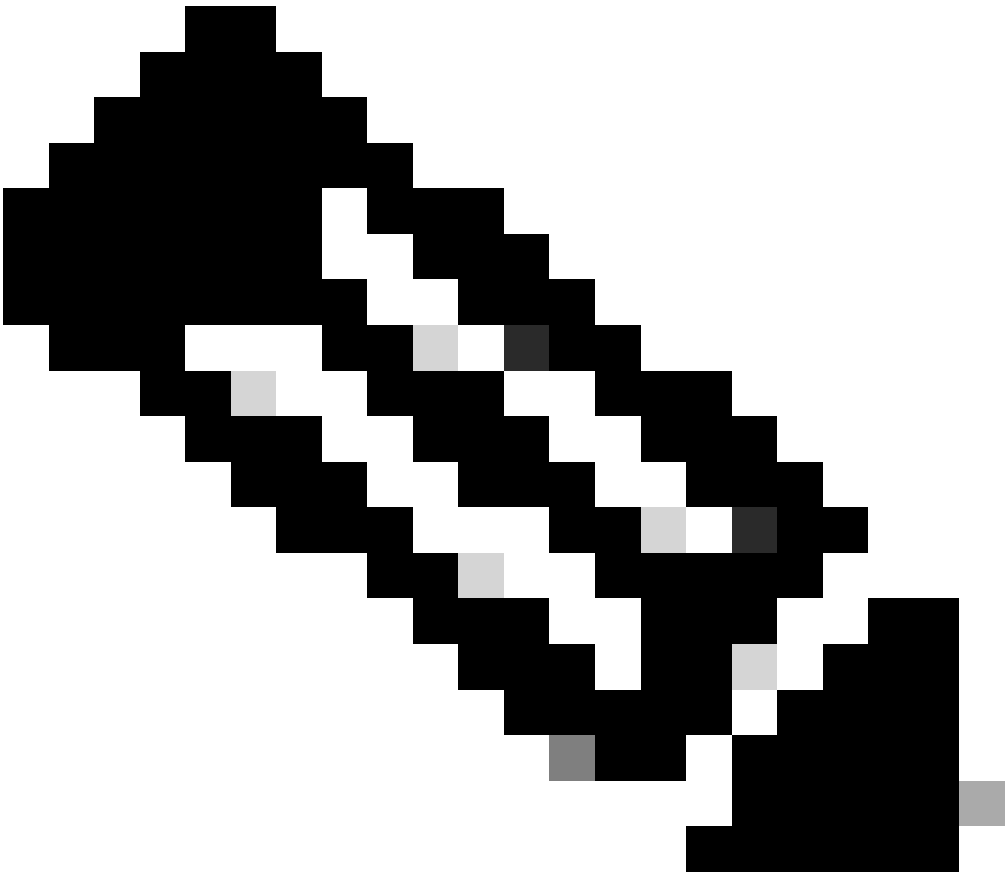
Configuración de firewall de host y creación de reglas

1. Navegue hastaAdministración > Firewall de host y haga clic enNueva configuración. 

   Firewall de host Nueva configuración

2. Seleccione un nombre y laAcción predeterminada. En este caso, seleccione Permitir. 

   Nombre de configuración y acción predeterminada del firewall del host

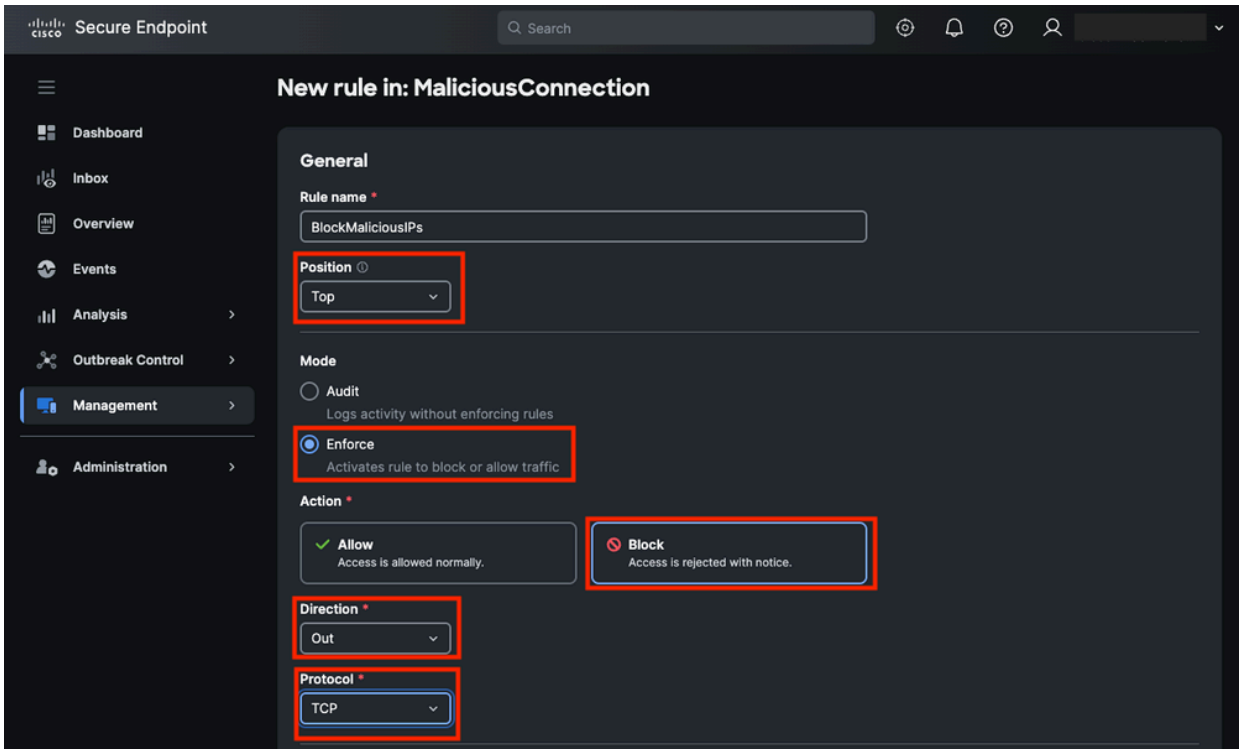


Nota: Tenga en cuenta que crea una regla de bloqueo, pero debe permitir que otro tráfico evite el impacto en conexiones legítimas.

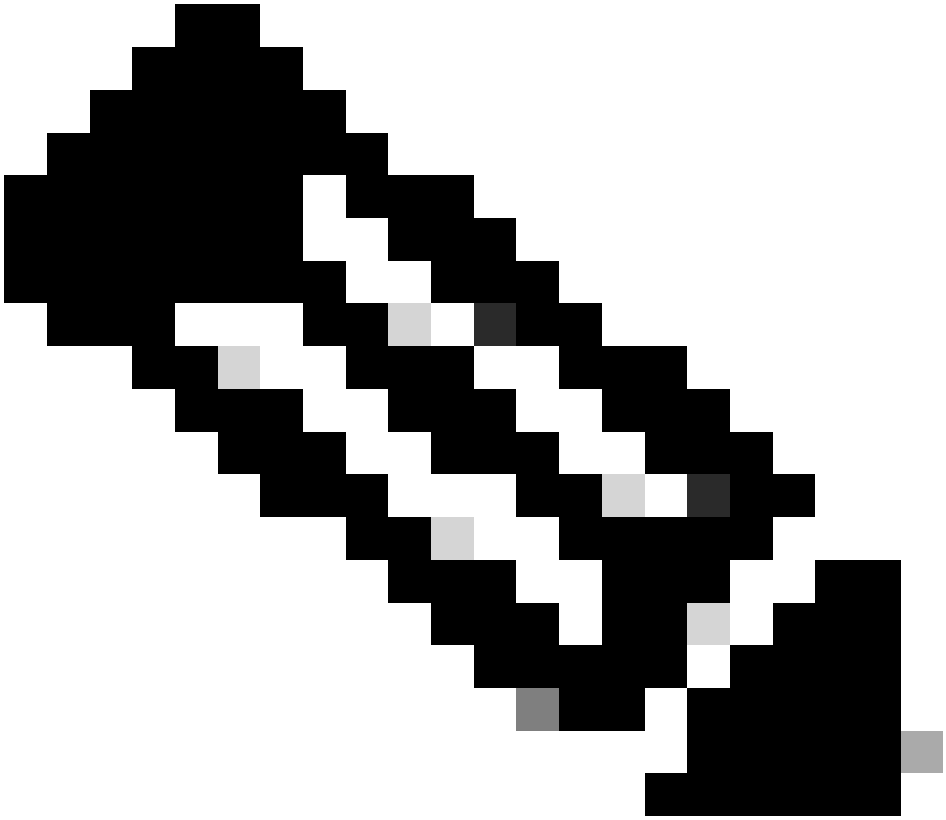
3. Compruebe que se ha creado la regla predeterminada y haga clic en Agregar regla. 

Agregar regla en el firewall host

4. Asigne un nombre y defina los siguientes parámetros:
    - Posición: Arriba
    - Modo: Aplicar
    - Acción: Bloqueo
    - Dirección: FUERA
    - Protocolo: TCP



Parámetros generales de regla



Nota: Cuando se trata de conexiones maliciosas desde un terminal interno a un destino externo, normalmente a Internet, la dirección siempre puede ser Out.

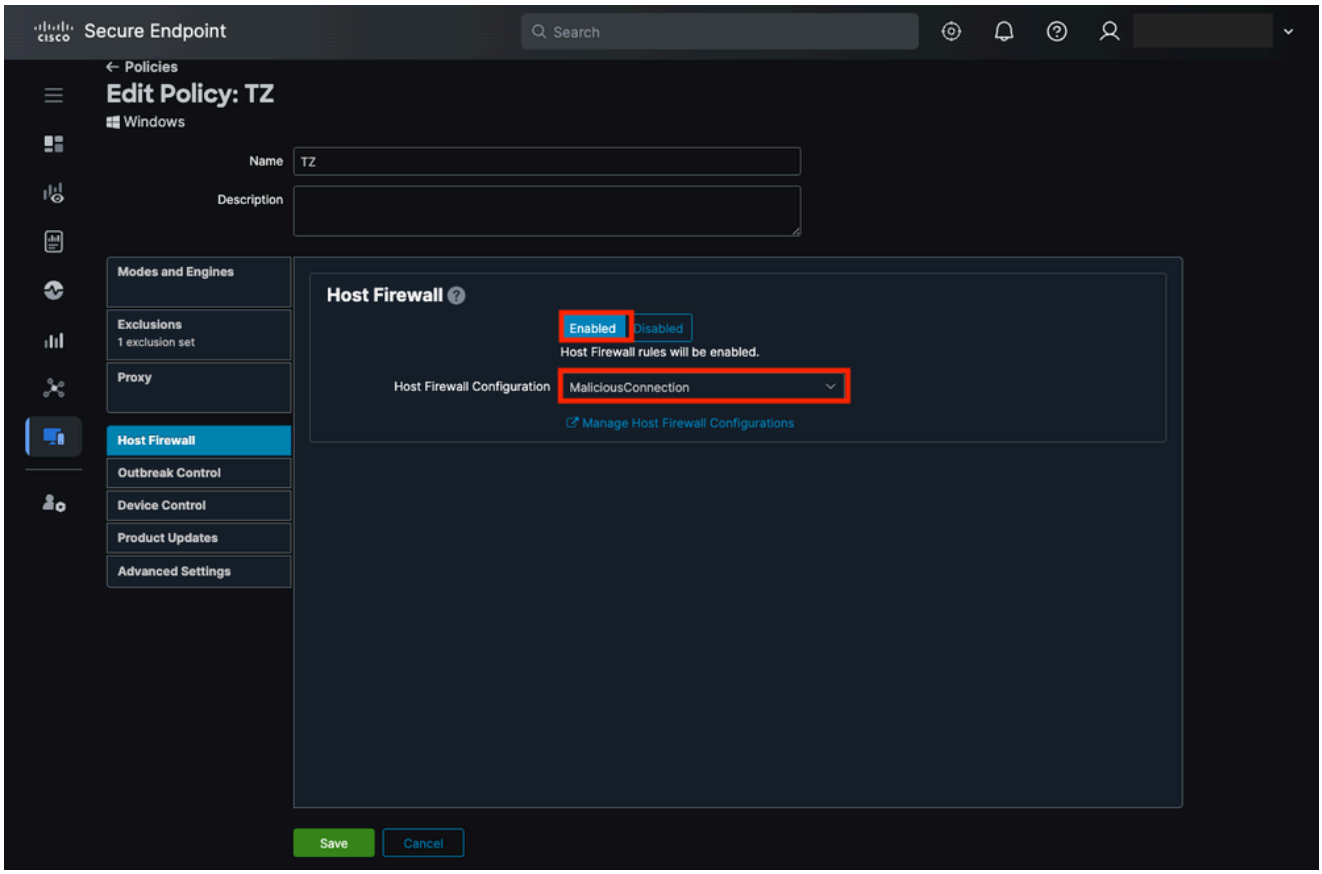
5. Especifique las direcciones IP locales y de destino:
   - IP local: 192.168.0.61
   - IP remota: 208.94.116.246
   - Deje el campoPuerto local en blanco.
   - Establezca el puerto de destino en 80 y 443, que corresponden a HTTP y HTTPS. 

     Direcciones y puertos de regla

6. Por último, haga clic en Guardar.

Habilitar el firewall de host en la directiva y asignar la nueva configuración

1. En Secure Endpoint Portal, navegue hasta Administración > Políticas y seleccione la política asociada al terminal en el que desea bloquear la actividad maliciosa.
2. Haga clic enEditar y desplácese a la fichaFirewall de host.
3. Habilite la función Host Firewall y seleccione la configuración reciente, en este caso MaliciousConnection.



Firewall de host habilitado en la directiva de terminales seguros

4. Click Save.

5. Finalmente, verifique que el terminal haya aplicado los cambios de política. 

Evento de actualización de directiva

Validar la configuración localmente

1. Utilice la URL malware.eicar.org en un navegador para confirmar que está bloqueada. 

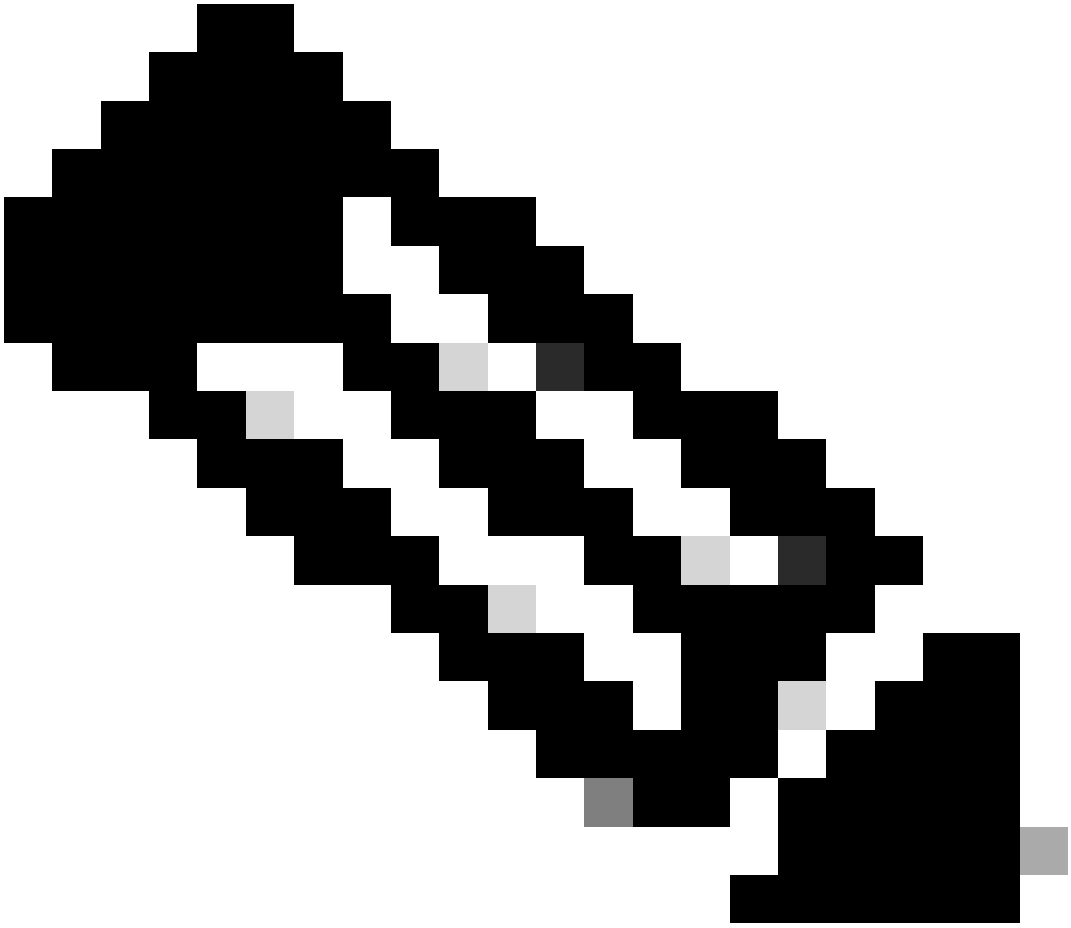
Error: acceso a la red denegado desde el explorador

2. Después de confirmar el bloque, verifique que no se haya establecido ninguna conexión. Utilice el comando netstat -ano | findstr ESTABLISHED para garantizar que la dirección IP asociada a la URL malintencionada (208.94.116.246) no sea visible.

Revisar registros

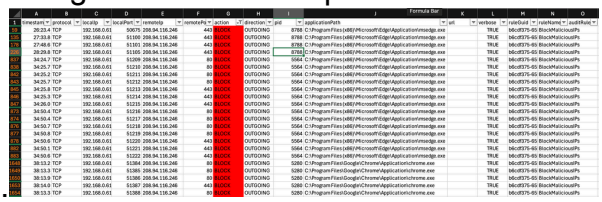
1. En el terminal, navegue hasta la carpeta:

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



Nota: El archivo de registro se encuentra en la carpeta <directorio de instalación>\Cisco\AMP\<versión del conector>\FirewallLog.csv

2. Abra el archivo CSV para validar las coincidencias de la regla de acción Bloquear. Utilice un filtro para distinguir entre permitir y bloquear conexiones.



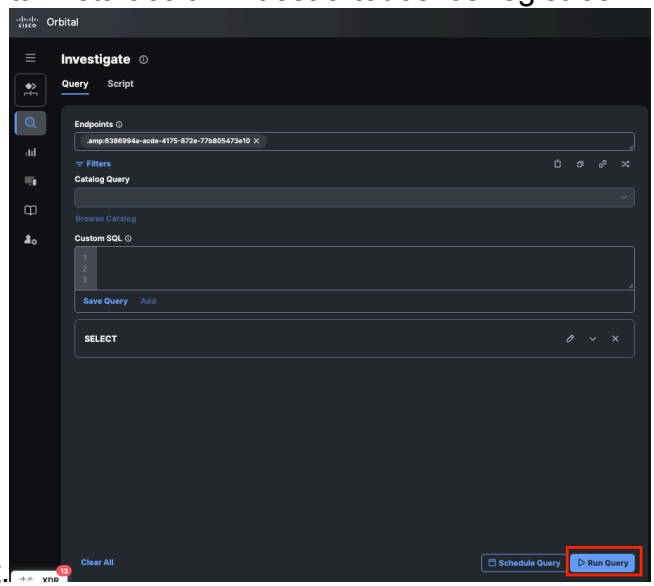
Registros del firewall en archivo CSV

Utilizar Orbital para recuperar registros de firewall

1. En Secure Endpoint Portal, navegue hasta Administración > Equipos, localice el terminal y haga clic en Recuperar registros de firewall en órbita. Esta acción le redirige al portal orbital.

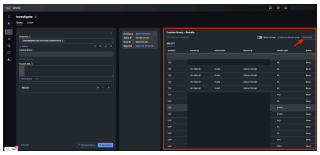
Botón para recuperar registros de firewall en órbita

2. En el portal orbital, haga clic en Ejecutar consulta. Esta acción muestra todos los registros grabados en el extremo para el firewall de host.



Ejecutar consulta desde órbita

3. La información está visible en la fichaResultados o puede descargarla.



Resultados de consulta desde orbital

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).