Dépannage d'une connexion malveillante avec le pare-feu hôte

Table des matières

Introduction

Ce document décrit comment détecter les connexions malveillantes sur un terminal Windows et les bloquer à l'aide du pare-feu hôte dans Cisco Secure Endpoint.

Conditions préalables

Exigences

- Le pare-feu hôte est disponible avec les packages Secure Endpoint Advantage et Premier.
- Versions de connecteur prises en charge
  - Windows (x64) : Connecteur Windows Secure Endpoint 8.4.2 et versions ultérieures.
  - Windows (ARM) : Connecteur Windows Secure Endpoint 8.4.4 et versions ultérieures.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

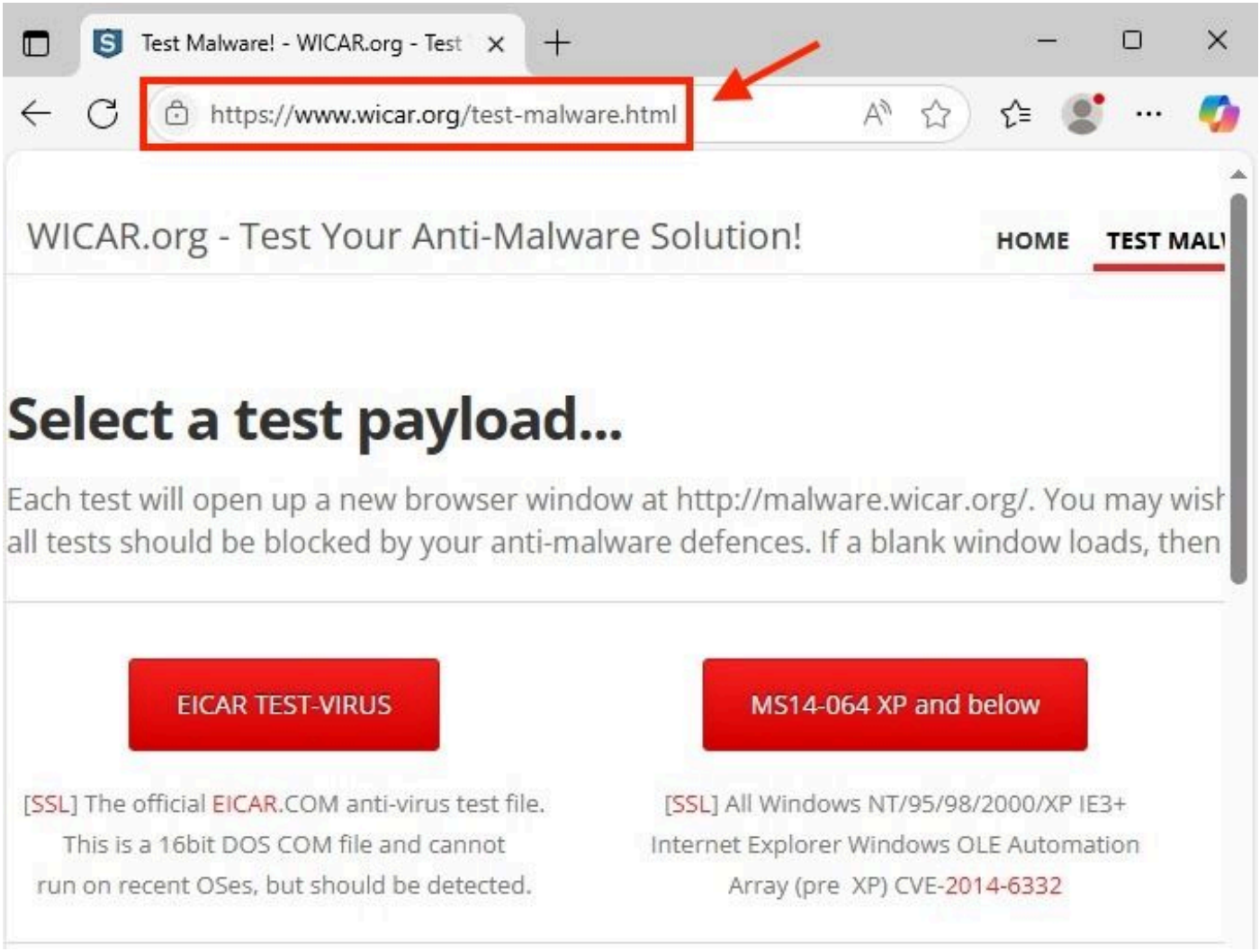
Guide de dépannage

Ce document fournit un guide pour bloquer les connexions malveillantes avec l'utilisation de Cisco

Secure Endpoint Host Firewall. Afin de tester, vous utilisez la page de test malware.wicar.org (208.94.116.246) pour créer un guide de dépannage.

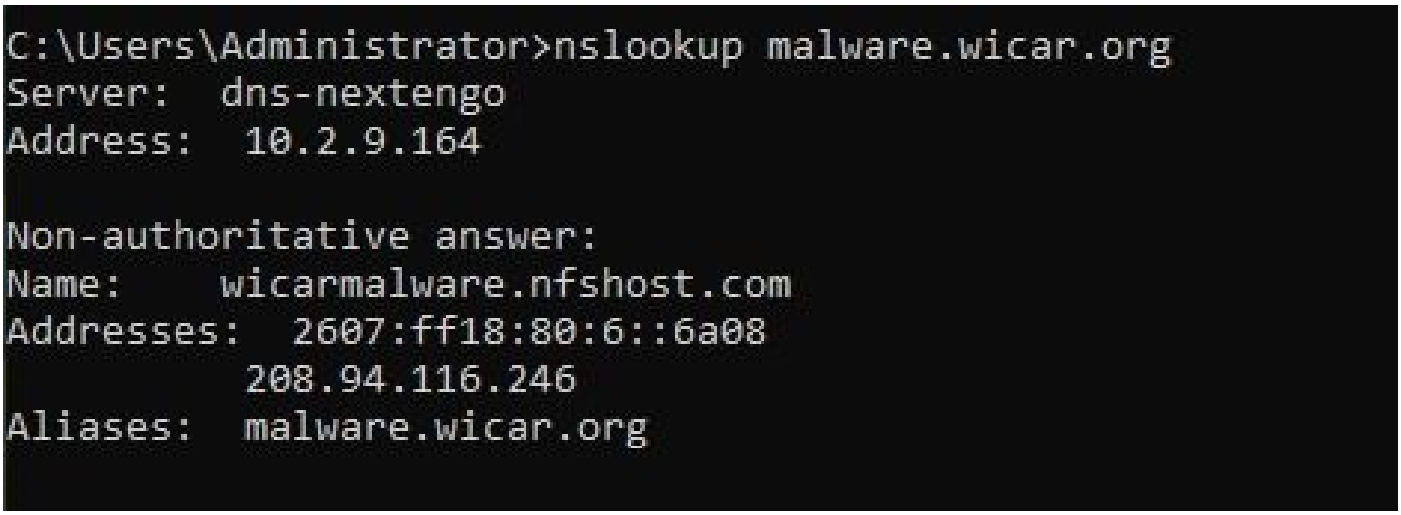
Étapes d'identification et de blocage des connexions malveillantes

1. Tout d'abord, vous devez identifier l'URL ou l'adresse IP que vous souhaitez vérifier et bloquer. Pour ce scénario, rendez-vous sur consider malware.wicar.org.
2. Vérifiez si l'accès à l'URL est successful. malware.wicar.org redirige vers une autre URL, comme indiqué dans l'image.



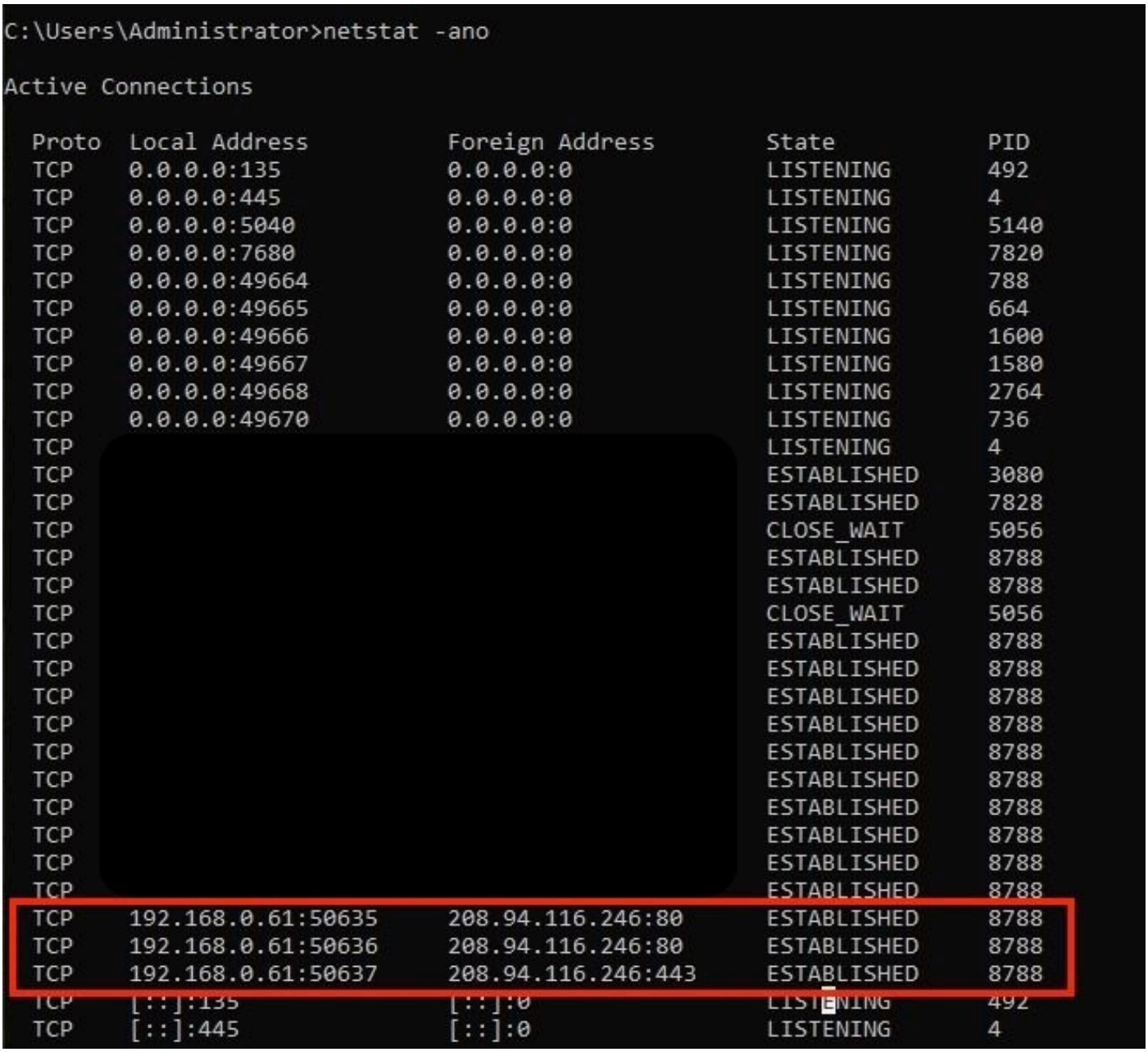
URL malveillante du navigateur

3. Utilisez la commande nslookup pour récupérer l'adresse IP associée à l'URL malware.wicar.org.



Sortie nslookup

4. Une fois l’adresse IP malveillante obtenue, vérifiez les connexions actives sur le point d’extrémité à l’aide de la commande : netstat -ano.



```
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
```

netstat pour toutes les connexions

5. Afin d'isoler les connexions actives, appliquez un filtre pour afficher uniquement les connexions établies.

```
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>
```

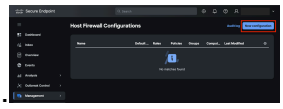
netstat pour les connexions établies

6. Recherchez l’adresse IP obtenue à l’aide de la commande lookup dans le résultat précédent. Identifiez l'IP source, l'IP de destination, le port source et le port de destination.

- Adresse IP locale : 192.168.0.61
- Adresse IP distante : 208.94.116.246
- Port local : Sans objet
- Port de destination 80 et 443

7. Une fois que vous avez ces informations, accédez au portail Cisco Secure Endpoint pour créer la configuration du pare-feu hôte.

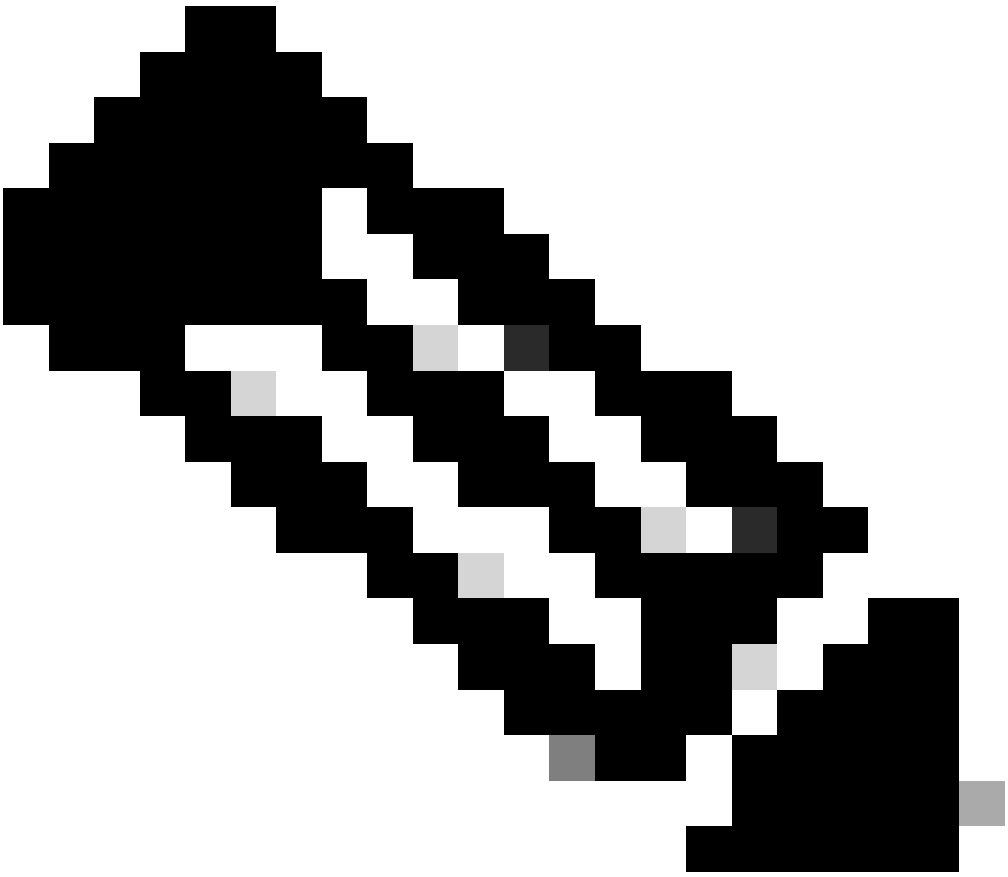
Configuration du pare-feu hôte et création de règles

1. Accédez à Management > Host Firewall et cliquez sur New Configuration. 

   Nouvelle configuration du pare-feu hôte

2. Sélectionnez un nom et l'action par défaut. Dans ce cas, sélectionnez Autoriser. 

   Nom de configuration du pare-feu hôte et action par défaut

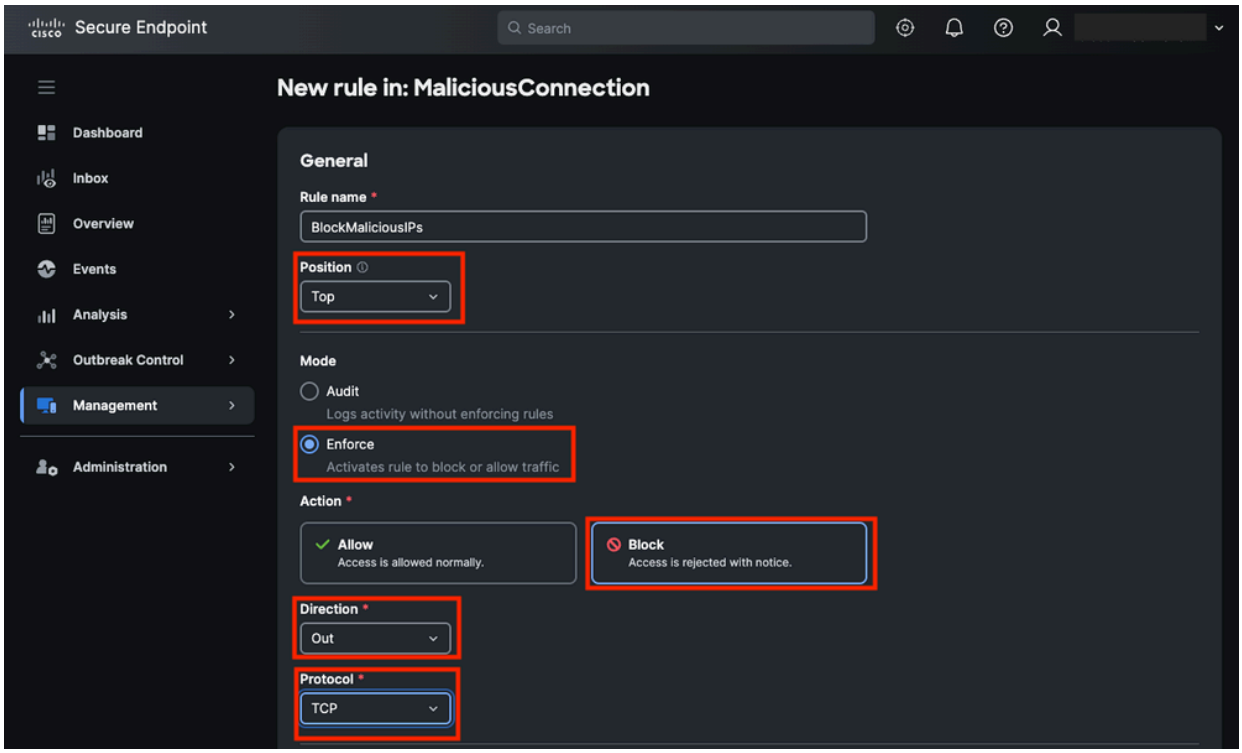


Remarque : Gardez à l'esprit que vous créez une règle de blocage, mais que vous devez autoriser d'autres trafics pour éviter d'avoir un impact sur les connexions légitimes.

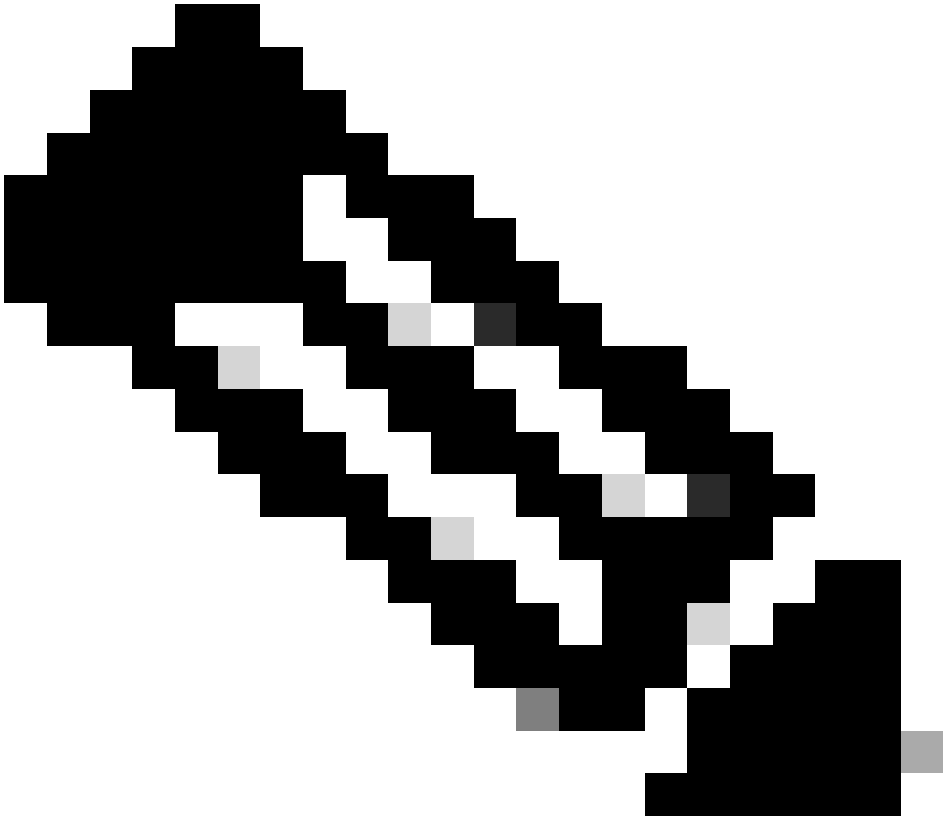
3. Vérifiez que la règle par défaut a été créée et cliquez sur Ajouter une règle.

Ajouter une règle dans le pare-feu hôte

4. Attribuez un nom et définissez les paramètres suivants :
    - Position : Haut
    - Mode : Appliquer
    - Action : Block
    - Direction: Dehors
    - Protocole : TCP

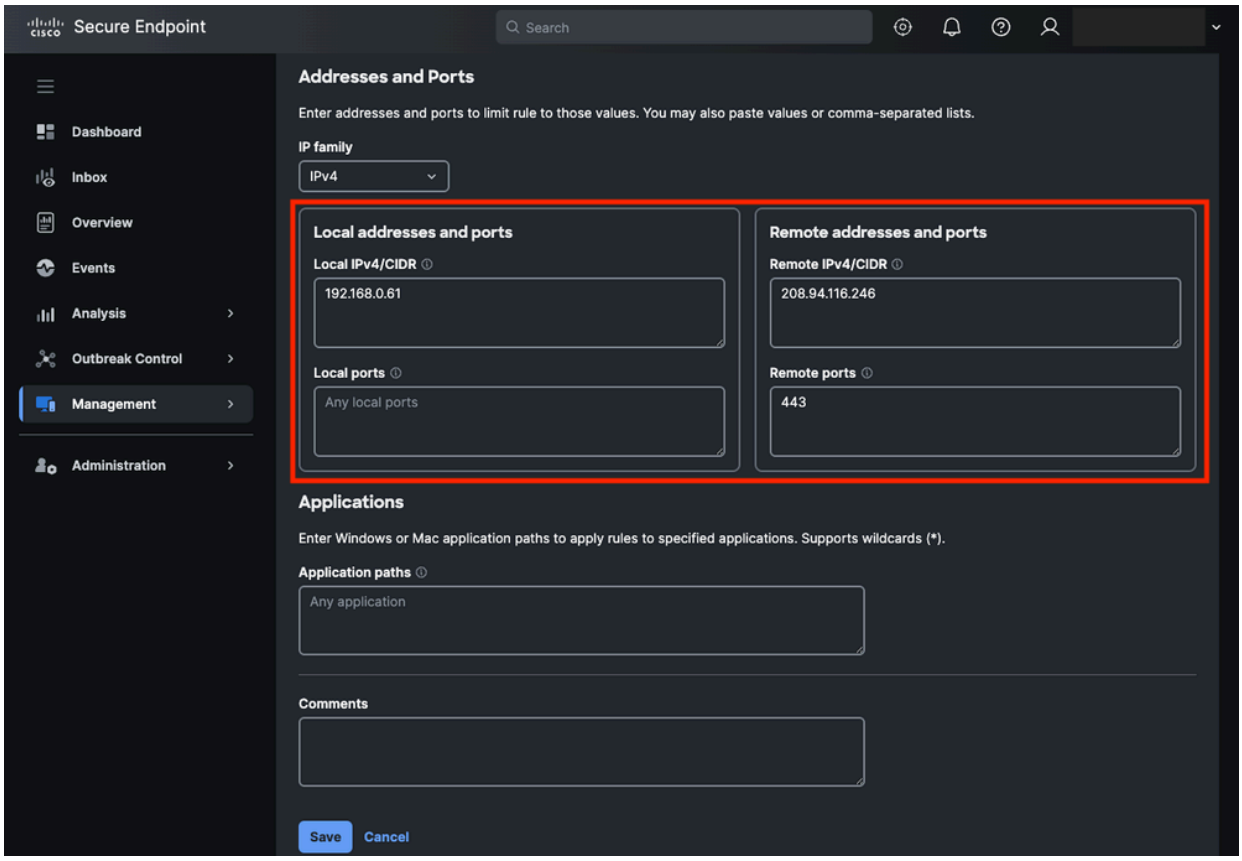


Paramètres généraux des règles



Remarque : Lorsque vous gérez des connexions malveillantes d'un terminal interne vers une destination externe, généralement vers Internet, la direction peut toujours être Out.

5. Spécifiez les adresses IP locales et de destination :
    - Adresse IP locale : 192.168.0.61
    - Adresse IP distante : 208.94.116.246
    - Ne renseignez pas le champ Local Port.
    - Définissez les ports de destination 80 et 443, ceux-ci correspondent à HTTP et HTTPS.

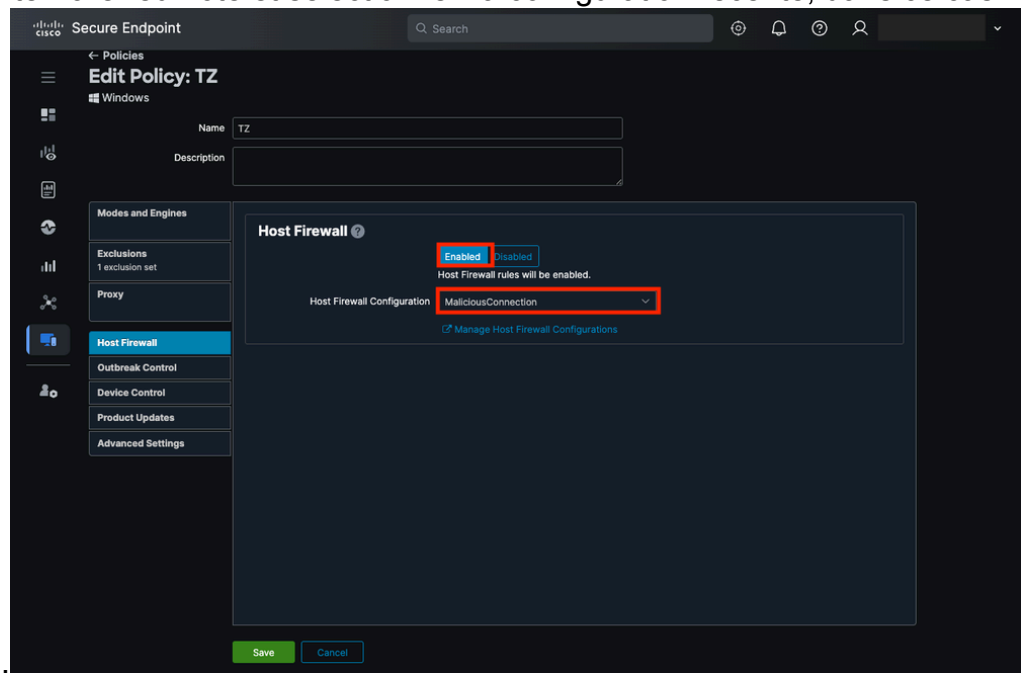


Adresses et ports de règle

6. Enfin, cliquez sur Enregistrer.

Activer le pare-feu hôte dans la stratégie et attribuer la nouvelle configuration

1. Dans Secure Endpoint Portal, accédez à Management > Policies et sélectionnez la stratégie associée au terminal où vous souhaitez bloquer les activités malveillantes.
2. Cliquez sur Modifier et accédez à l'onglet Pare-feu hôte.
3. Activez la fonctionnalité Pare-feu hôte et sélectionnez la configuration récente, dans ce cas MaliciousConnection.



Pare-feu hôte activé dans la stratégie de point de terminaison sécurisé

4. Cliquez sur Save.
5. Enfin, vérifiez que le point de terminaison a appliqué les modifications de stratégie. 

Événement de mise à jour de stratégie

Validation locale de la configuration

1. Utilisez l'URL malware.eicar.org dans un navigateur pour confirmer qu'il est bloqué. 

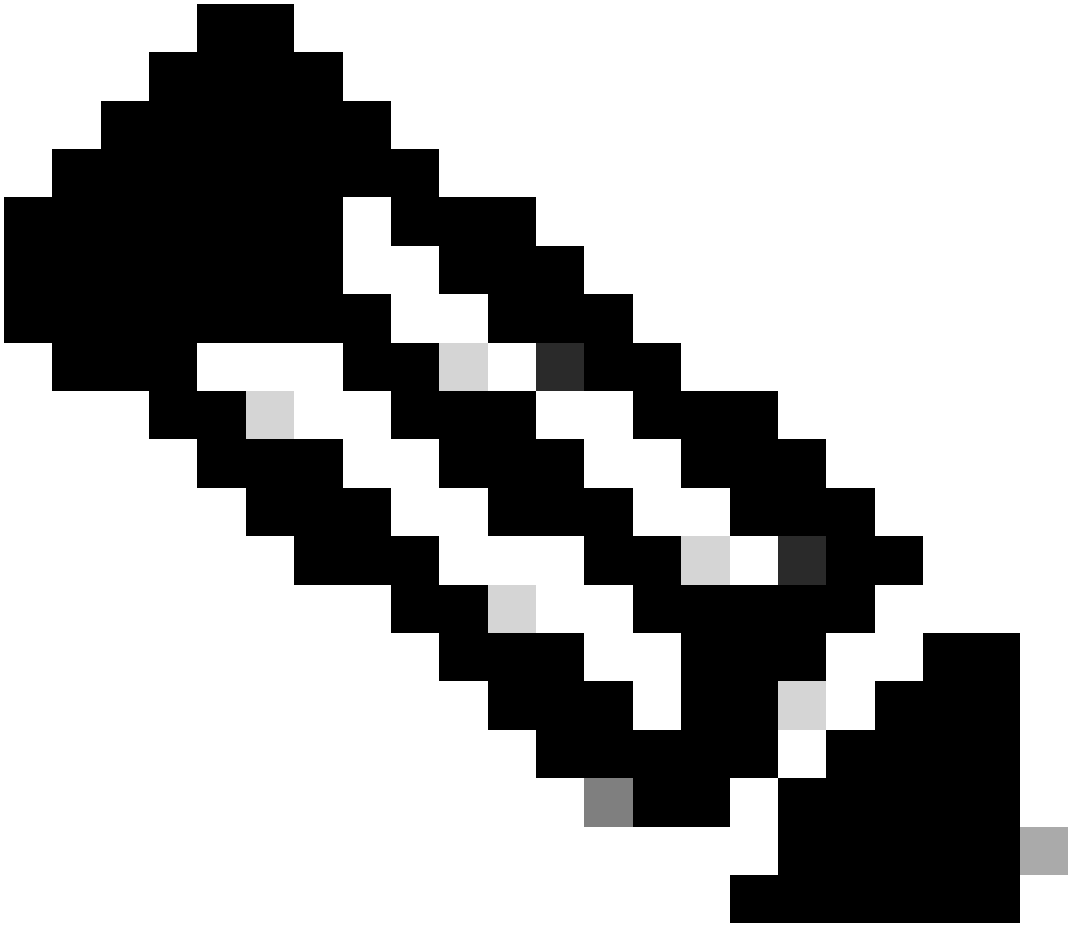
Erreur Accès réseau refusé depuis le navigateur

2. Après avoir confirmé le blocage, vérifiez qu'aucune connexion n'est établie. Utilisez la commande netstat -ano | findstr ÉTABLI pour s'assurer que l'adresse IP associée à l'URL malveillante (208.94.116.246) n'est pas visible.

Consulter les journaux

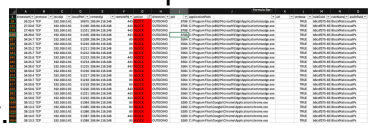
1. Sur le point de terminaison, accédez au dossier :

C:\Program Files\Cisco\AMP\<Version du connecteur>\FirewallLog.csv



Remarque : Le fichier journal se trouve dans le dossier <répertoire d'installation>\Cisco\AMP\<Version du connecteur>\FirewallLog.csv

2. Ouvrez le fichier CSV pour valider les correspondances pour la règle d'action Bloquer. Utilisez un filtre pour faire la distinction entre les connexions Autoriser et Bloquer.



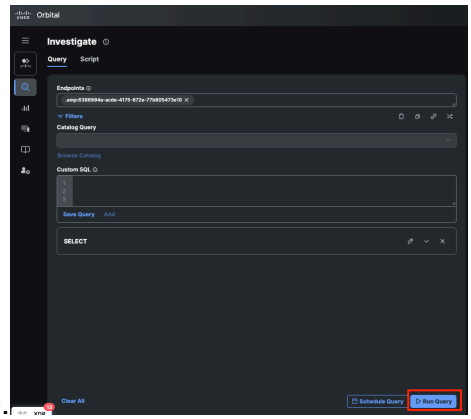
Journaux de pare-feu dans le fichier CSV

Utiliser Orbital pour récupérer les journaux de pare-feu

1. Dans Secure Endpoint Portal, accédez à Management > Computers, localisez le terminal et cliquez sur Retrieve Firewall Logs in Orbital. Cette action vous redirige vers le portail orbital.

Bouton de récupération des journaux de pare-feu en orbite

2. Dans le portail orbital, cliquez sur Exécuter la requête. Cette action affiche tous les journaux

enregistrés sur le point de terminaison pour le pare-feu hôte. 

Exécuter la requête à partir de l'orbite

3. Les informations sont visibles dans l'onglet Résultats ou vous pouvez les télécharger. 

Résultats de la requête Orbital

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.