Problemen met schadelijke verbindingen met hostfirewall oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u schadelijke verbindingen op een Windows-eindpunt kunt detecteren en blokkeren met de hostfirewall in Cisco Secure Endpoint.

Voorwaarden

Vereisten

- Host Firewall is beschikbaar met Secure Endpoint Advantage- en Premier-pakketten.
- Ondersteunde connectorversies
  - Windows (x64): Secure Endpoint Windows-connector 8.4.2 en hoger.
  - Windows (ARM): Secure Endpoint Windows-connector 8.4.4 en hoger.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

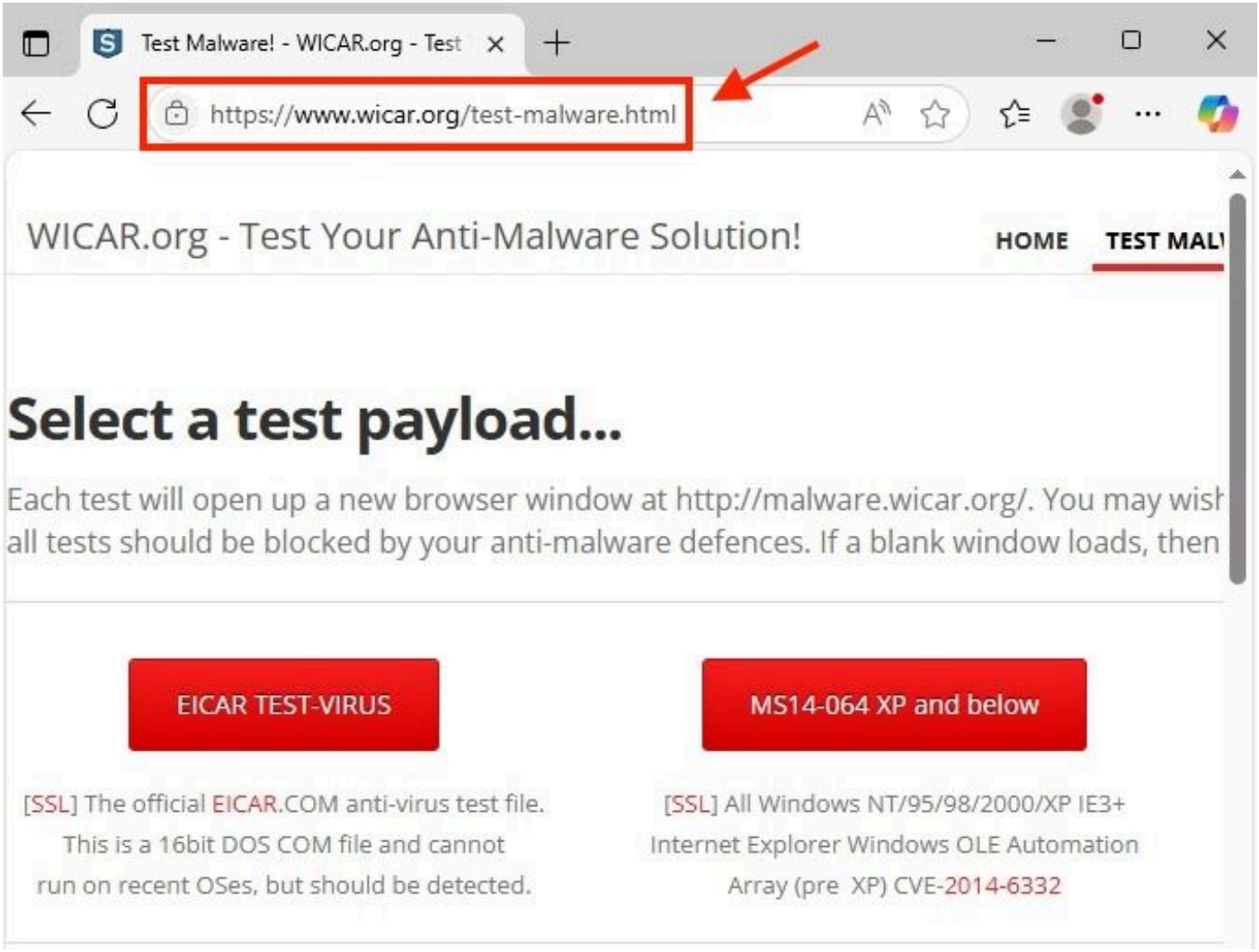
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Gids voor probleemoplossing

Dit document biedt een handleiding voor het blokkeren van schadelijke verbindingen met het gebruik van Cisco Secure Endpoint Host Firewall. Om te testen, gebruikt u de testpagina malware.wicar.org (208.94.116.246) om een handleiding voor probleemoplossing te maken.

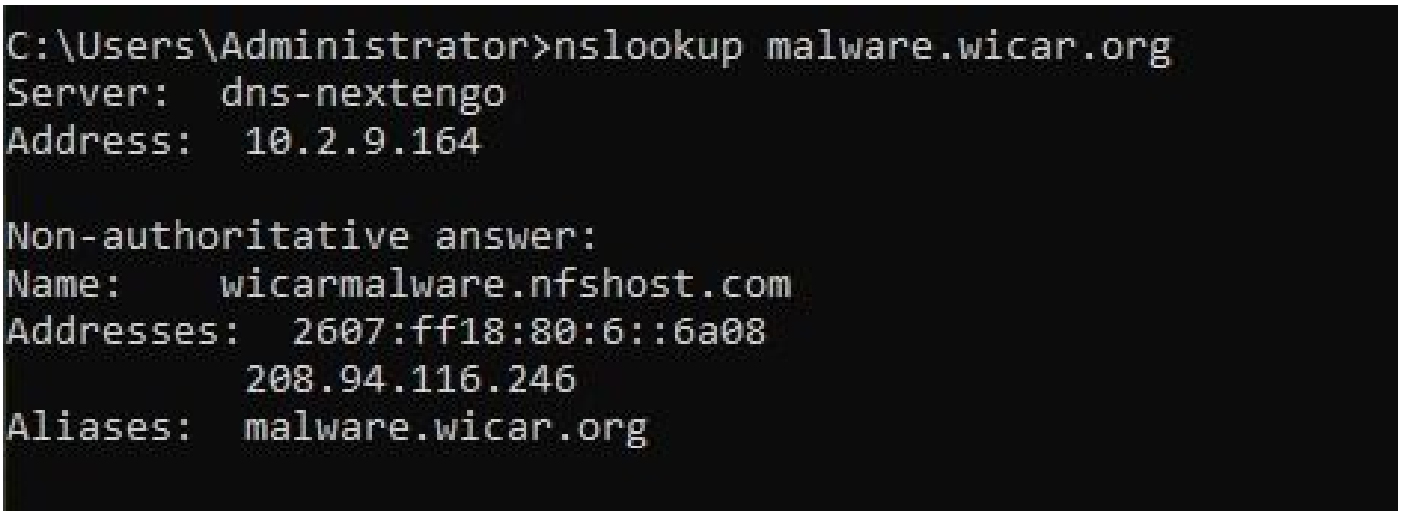
Stappen voor het identificeren en blokkeren van schadelijke verbindingen

1. Eerst moet u de URL of het IP-adres identificeren dat u wilt bekijken en blokkeren. Kijk voor dit scenario naar malware.wicar.org.
2. Controleer of de toegang tot de URL succesvol is. malware.wicar.org verwijst door naar een andere URL, zoals in de afbeelding wordt weergegeven.



Kwaadaardige URL van browser

3. Gebruik de opdracht nslookup om het IP-adres op te halen dat is gekoppeld aan de URL malware.wicar.org.



nslookup-uitvoer

4. Zodra het schadelijke IP-adres is verkregen, controleert u de actieve verbindingen op het eindpunt met de opdracht: 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 voor alle aansluitingen

5. Om actieve verbindingen te isoleren, past u een filter toe om alleen gevestigde verbindingen weer te geven.

```
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 voor gevestigde verbindingen

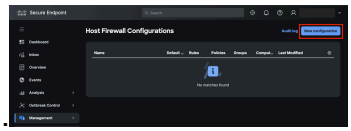
6. Zoek het IP-adres dat is verkregen met de opdracht lookup in de vorige uitvoer. Identificeer de bron-IP, bestemming-IP, bronpoort en bestemmingspoort.

- Lokaal IP: 192.168.0.61
- Extern IP: 208.94.116.246
- Lokale poort: niet van toepassing
- Bestemming Porto 80 en 443

7. Zodra u over deze informatie beschikt, navigeert u naar het Cisco Secure Endpoint Portal om de hostfirewallconfiguratie te maken.

Configuratie van firewall en maken van regels voor host

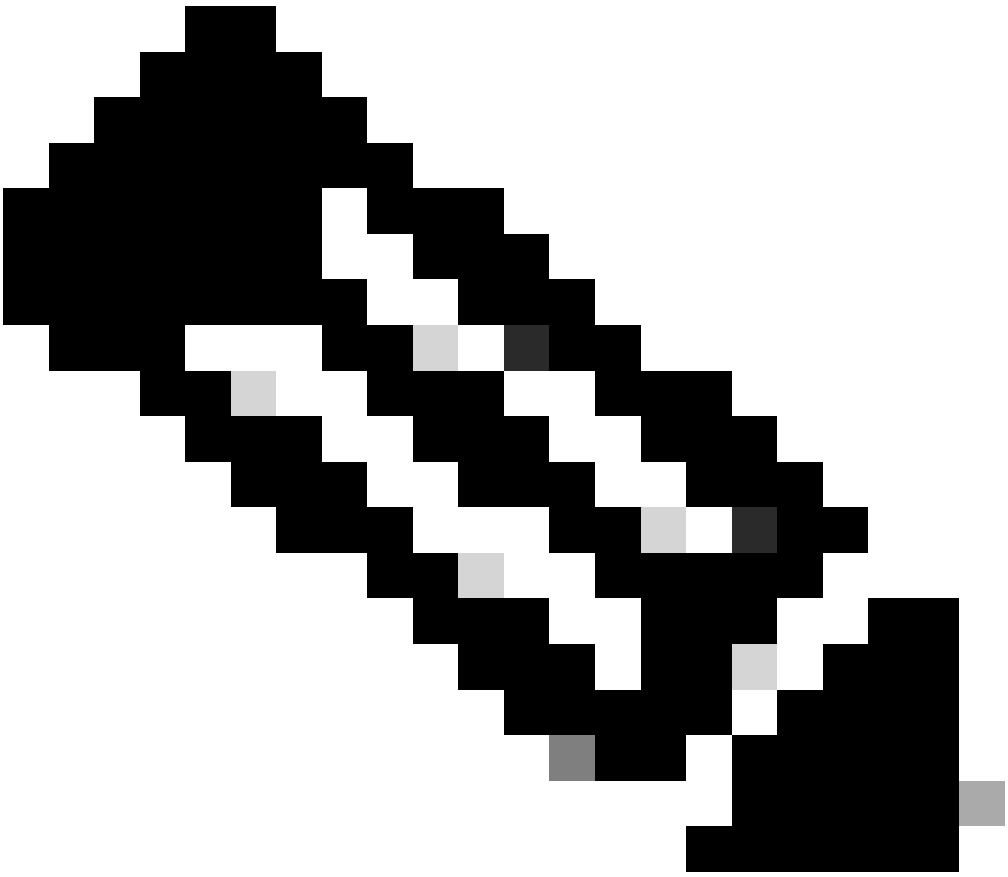
1. Navigeer naar Beheer > Host Firewall en klik op Nieuwe configuratie.



Host Firewall Nieuwe configuratie

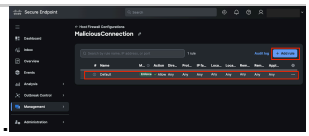
2. Selecteer een naam en de standaardactie. Selecteer in dit geval Toestaan.

Naam en standaardactie van de configuratie van de hostfirewall



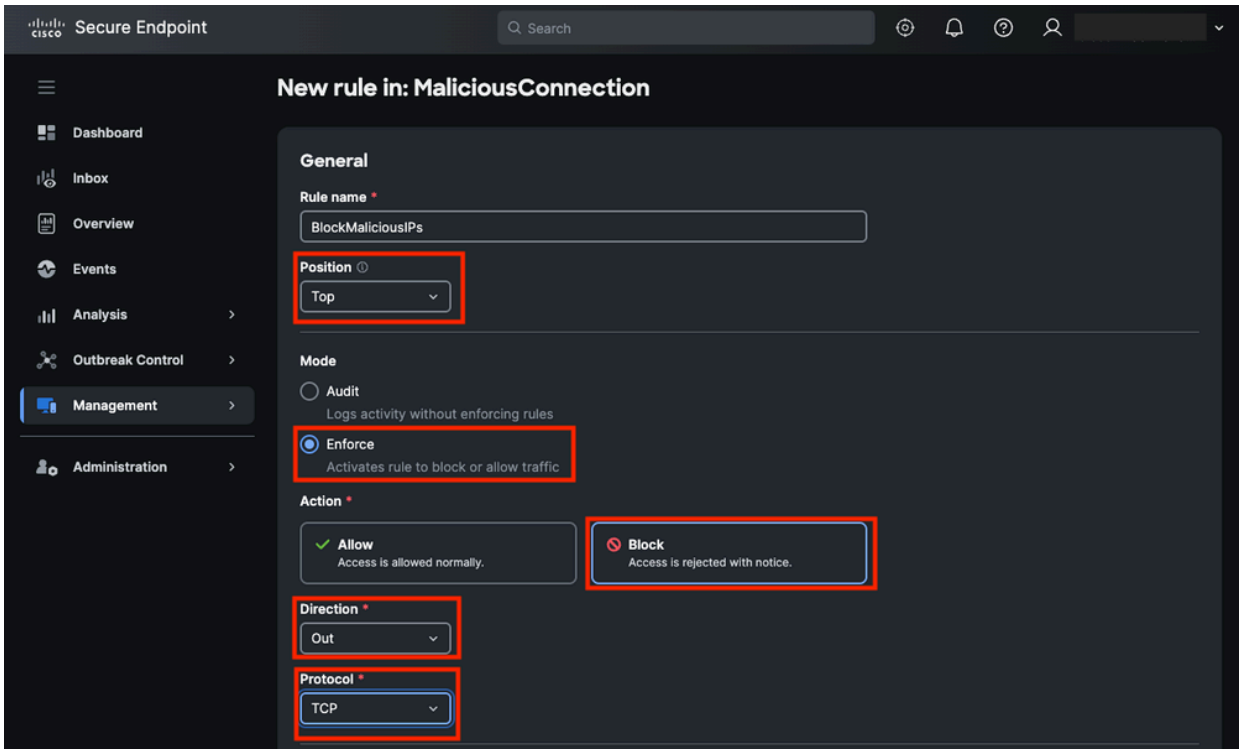
Opmerking: houd er rekening mee dat u een blokregel maakt, maar dat u ander verkeer moet toestaan om impact op legitieme verbindingen te voorkomen.

3. Controleer of de standaardregel is gemaakt en klik op Regel toevoegen.

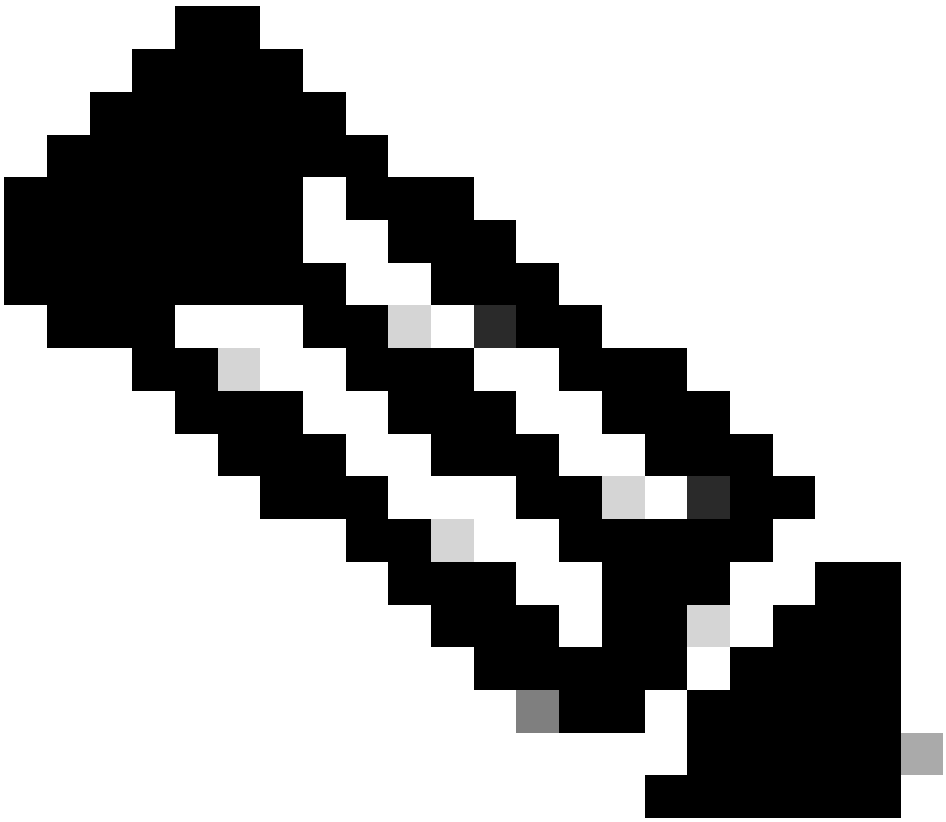


Regel toevoegen in hostfirewall

4. Wijs een naam toe en stel de volgende parameters in:
    - Positie: boven
    - Modus: afdwingen
    - Actie: blokkeren
    - Richting: Uit
    - Protocol: TCP

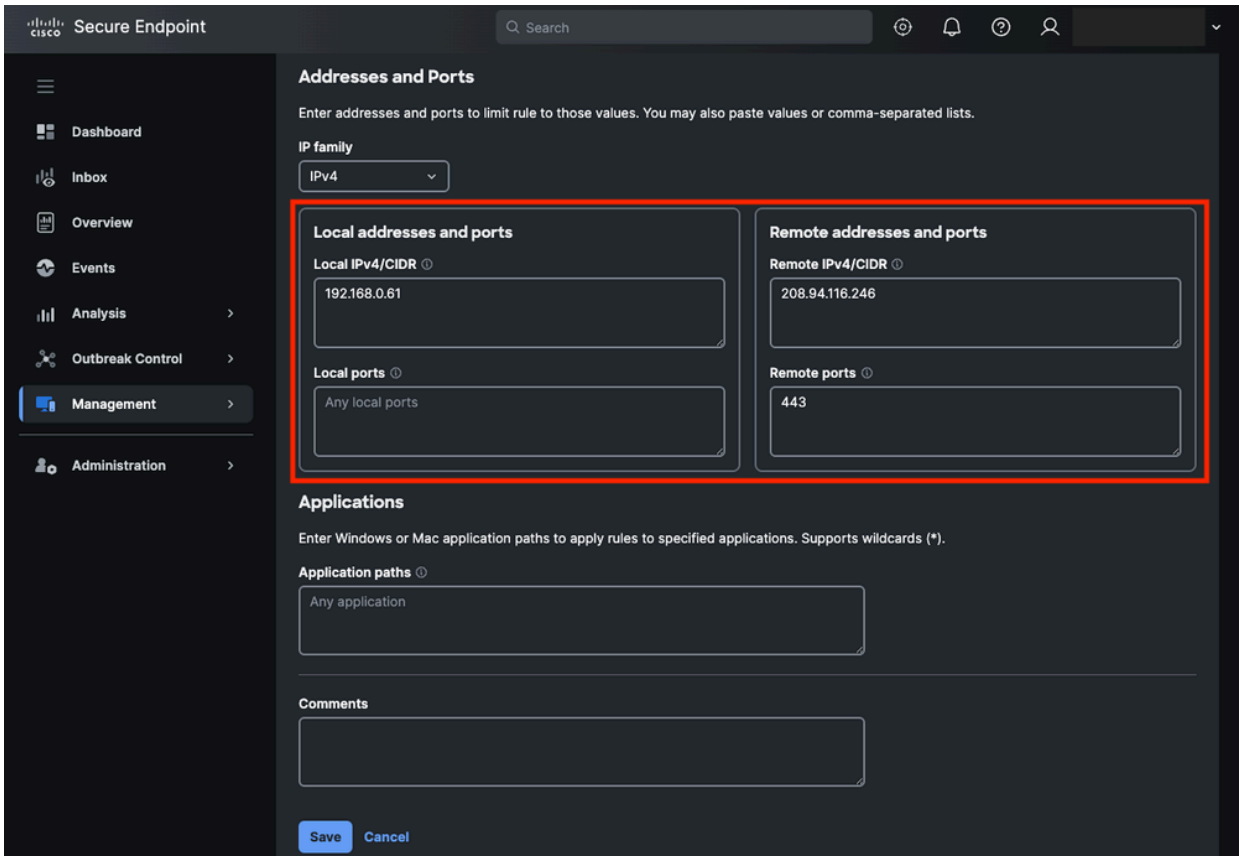


Algemene parameters regel



Opmerking: wanneer u schadelijke verbindingen van een intern eindpunt naar een externe bestemming adresseert, meestal naar het internet, kan de richting altijd uit zijn.

5. Geef de lokale en bestemmings-IP's op:
    - Lokaal IP: 192.168.0.61
    - Extern IP: 208.94.116.246
    - Laat het lokale Portfield leeg.
    - Stel de bestemmingspoort in op 80 en 443, deze komen overeen met HTTP en HTTPS.

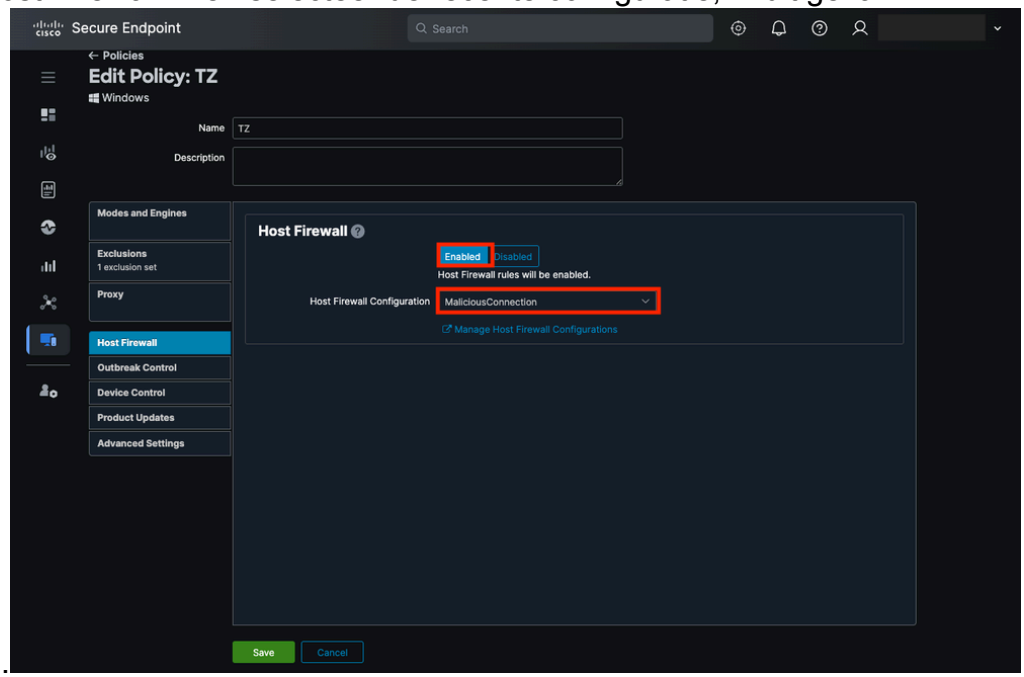


Regel Adressen en poorten

6. Klik ten slotte op Opslaan.

Host Firewall inschakelen in het beleid en de nieuwe configuratie toewijzen

1. Navigeer in het Secure Endpoint Portal naar Beheer > Beleid en selecteer het beleid dat is gekoppeld aan het eindpunt waar u schadelijke activiteiten wilt blokkeren.
2. Klik op Bewerken en navigeer naar het tabblad Host Firewall.
3. Schakel de functie Host Firewall in en selecteer de recente configuratie, in dit geval MaliciousConnection.



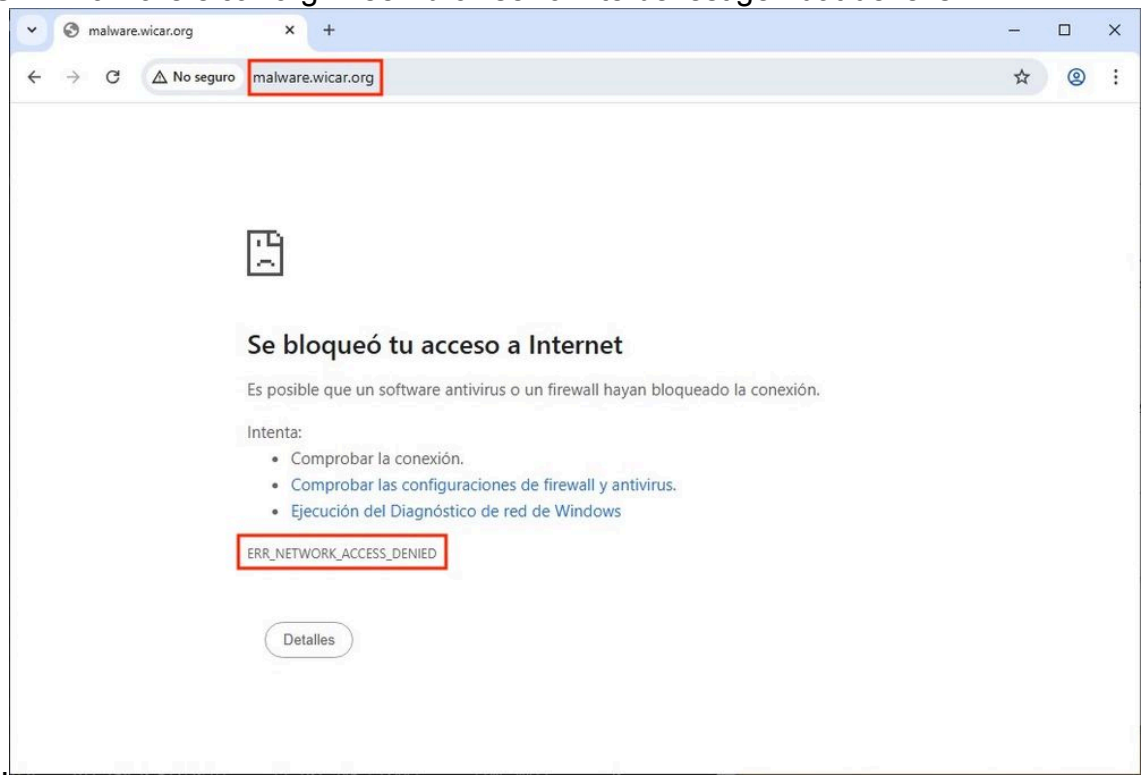
Hostfirewall ingeschakeld in beleid voor beveiligd eindpunt

4. Klik op Save (Opslaan).

5. Controleer ten slotte of het eindpunt de beleidswijzigingen heeft toegepast. 

Policy Update Event

De configuratie lokaal valideren

1. Gebruik de URL malware.eicar.org in een browser om te bevestigen dat deze is geblokkeerd. 

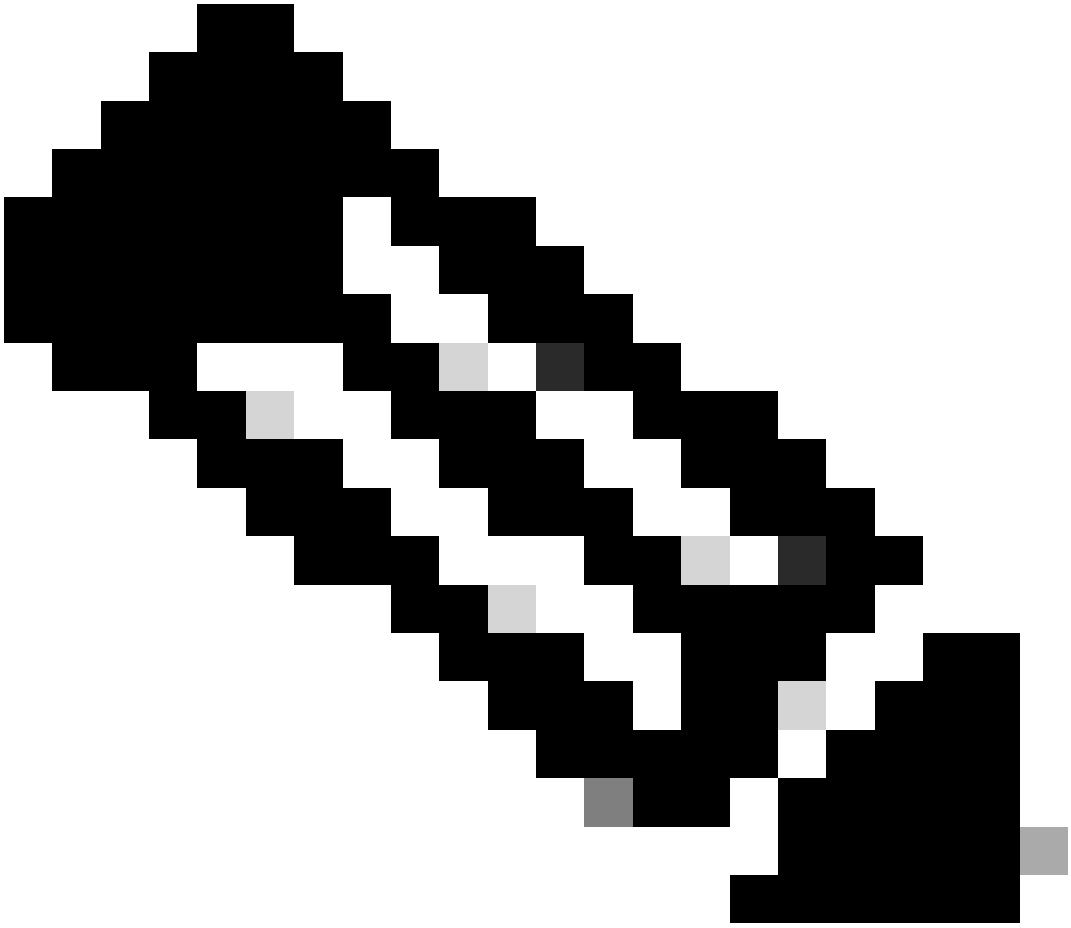
Fout bij netwerktoegang geweigerd vanuit browser

2. Controleer of er geen verbindingen tot stand zijn gebracht nadat u de blokkering hebt bevestigd. Gebruik de opdracht netstat -ano | findstr ESTABLISHED om ervoor te zorgen dat het IP-adres dat is gekoppeld aan de schadelijke URL (208.94.116.246) niet zichtbaar is.

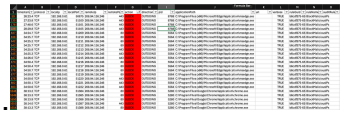
Logbestanden bekijken

1. Navigeer op het eindpunt naar de map:

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



Opmerking: Het logbestand bevindt zich in de map <install directory>\Cisco\AMP\<Connector version>\FirewallLog.csv

2. Open het CSV-bestand om overeenkomsten voor de actieregel Blok te valideren. Gebruik een filter om onderscheid te maken tussen verbindingen toestaan en blokkeren. 

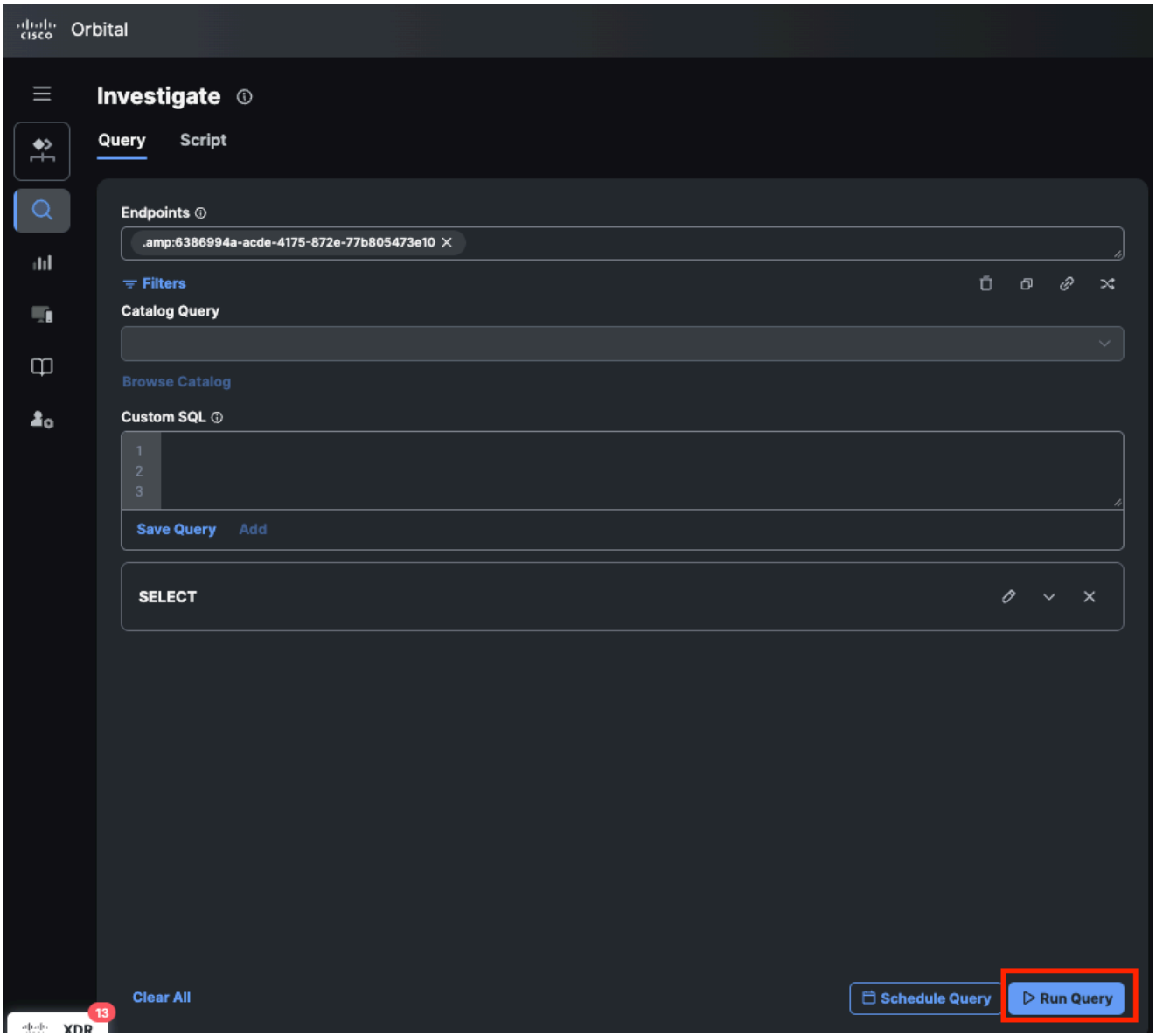
Firewall logt in CSV-bestand

Orbital gebruiken om firewalllogboeken op te halen

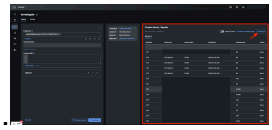
1. Navigeer in het Secure Endpoint Portal naar Beheer > Computers, zoek het eindpunt en klik op Firewall-logboeken ophalen in Orbital. Deze actie leidt je door naar het Orbital Portal. 

   Knop om firewalllogboeken in Orbital op te halen

2. Klik in het Orbital Portal op Query uitvoeren. Met deze actie worden alle logs weergegeven die zijn opgenomen op het eindpunt voor de hostfirewall.



Query vanuit orbitaal uitvoeren

3. De informatie is zichtbaar in de resultatenbalk, of u kunt deze downloaden. 

Zoekresultaten van Orbital

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.