Risoluzione dei problemi di connessione dannosa con il firewall host

Sommario

Introduzione

In questo documento viene descritto come rilevare connessioni dannose su un endpoint Windows e bloccarle utilizzando Host Firewall in Cisco Secure Endpoint.

Prerequisiti

Requisiti

- Il firewall host è disponibile con i pacchetti Secure Endpoint Advantage e Premier.
- Versioni dei connettori supportate
  - Windows (x64): Secure Endpoint Windows Connector 8.4.2 e versioni successive.
  - Finestre (ARM): Secure Endpoint Windows Connector 8.4.4 e versioni successive.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

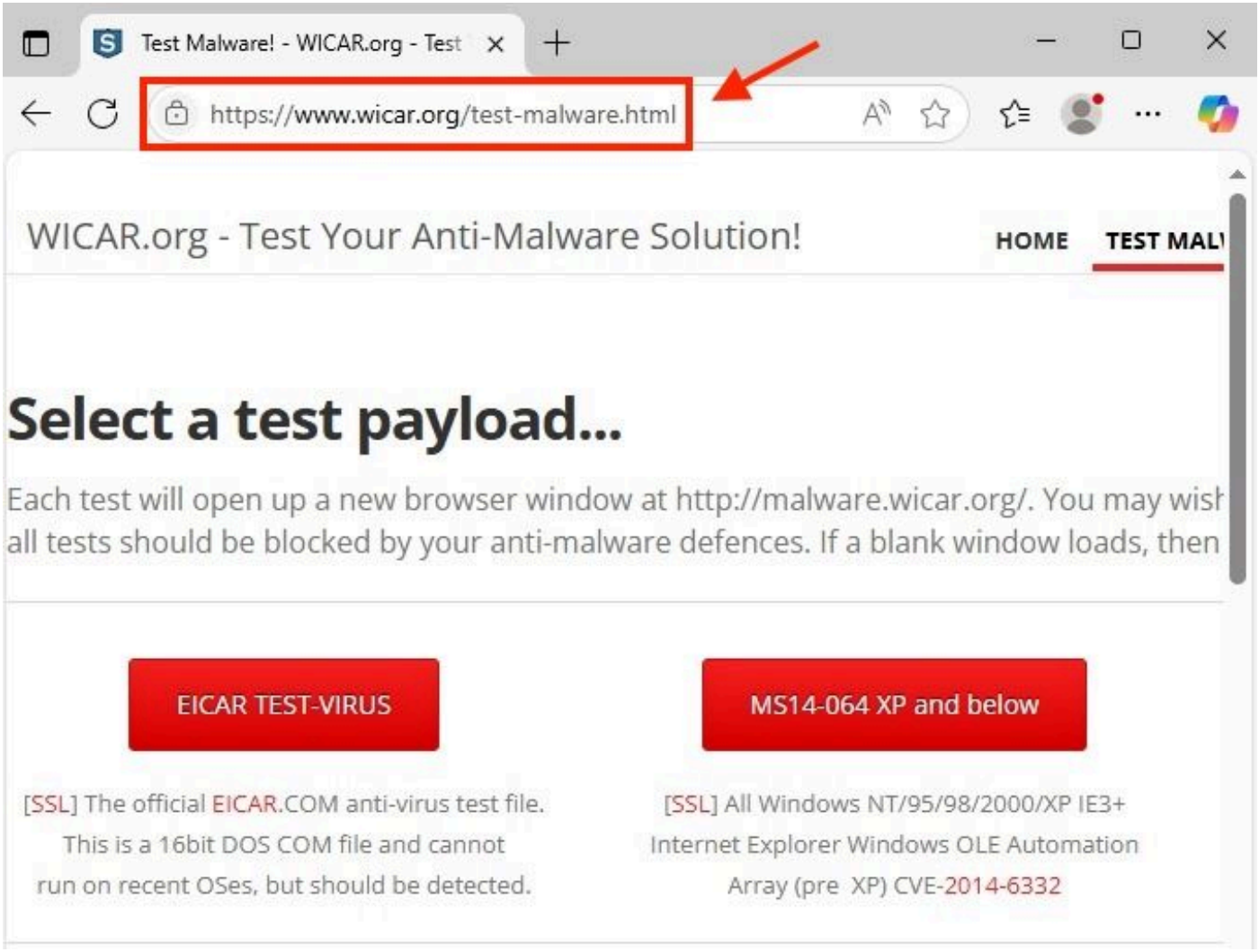
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Guida alla risoluzione dei problemi

In questo documento viene fornita una guida per bloccare connessioni dannose con l'uso di Cisco Secure Endpoint Host Firewall. Per eseguire il test, utilizzare la pagina di prova malware.wicar.org (208.94.116.246) per creare una guida alla risoluzione dei problemi.

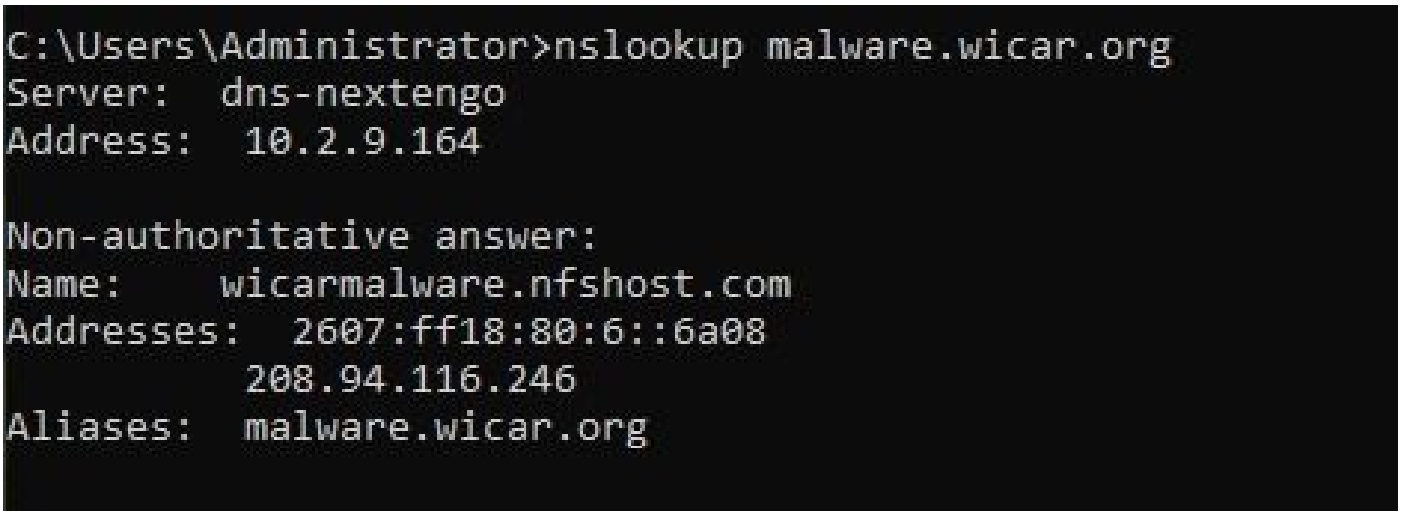
Procedure per identificare e bloccare le connessioni dannose

1. Innanzitutto, è necessario identificare l'URL o l'indirizzo IP che si desidera esaminare e bloccare. Per questo scenario consider malware.wicar.org.
2. Verificare se l'accesso all'URL è successful. malware.wicar.org reindirizza a un URL diverso, come mostrato nell'immagine.



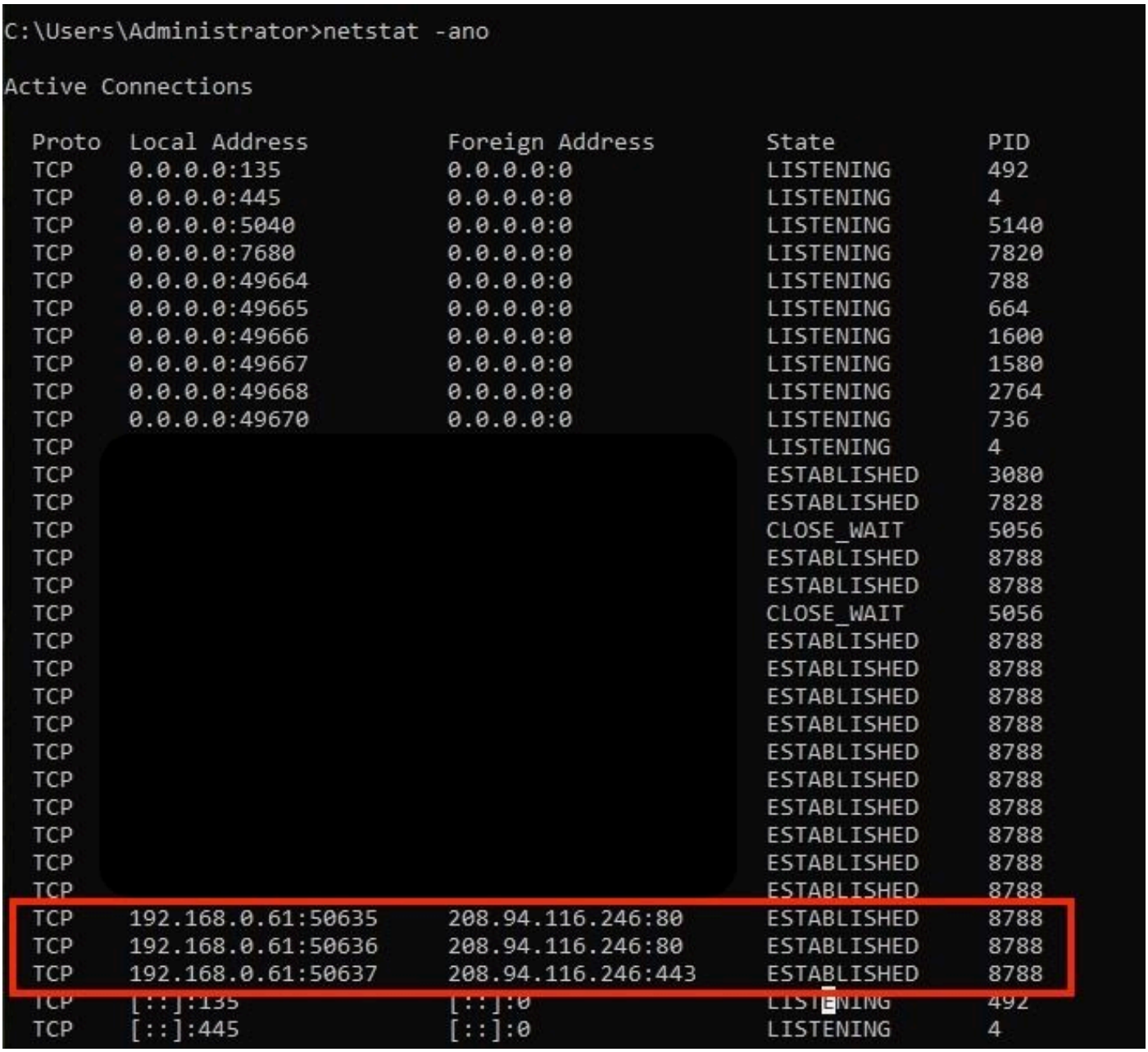
URL dannoso del browser

3. Utilizzare il comando nslookup per recuperare l'indirizzo IP associato all'URL malware.wicar.org.



Output nslookup

4. Dopo aver ottenuto l'indirizzo IP dannoso, controllare le connessioni attive sull'endpoint con il comando:netstat -ano.



netstat per tutte le connessioni

5. Per isolare le connessioni attive, applicare un filtro per visualizzare solo le connessioni stabilite.

```
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>
```

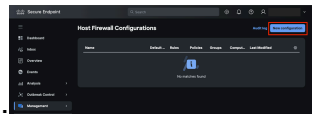
netstat per le connessioni stabilite

6. Cercare l'indirizzo IP ottenuto dal comando lookupnell'output precedente. Identificare l'IP di origine, di destinazione, di origine e di destinazione.

- IP locale: 192.168.0.61
- IP remoto: 208.94.116.246
- Porta locale: Non applicabile
- Porta di destinazione 80 e 443

7. Dopo aver ottenuto queste informazioni, passare al Cisco Secure Endpoint Portal per creare la configurazione del firewall host.

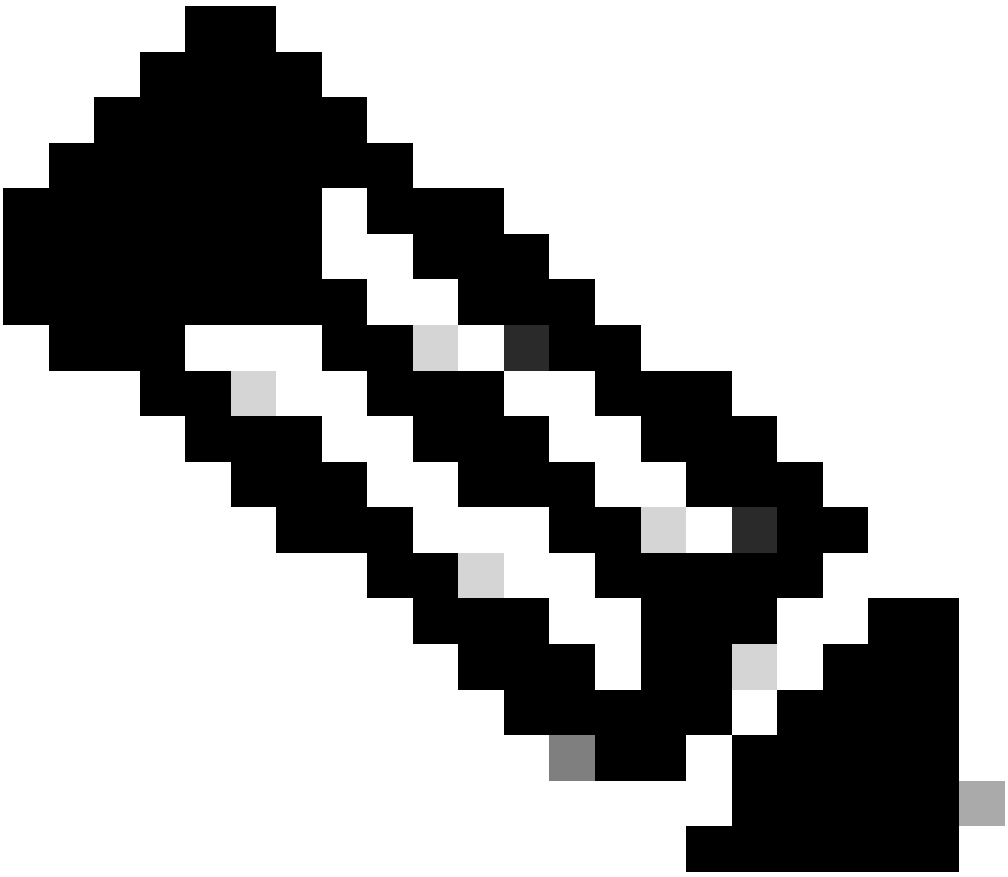
Configurazione del firewall host e creazione di regole

1. Passare a Gestione > Firewall host e fare clic su Nuova configurazione. 

   Nuova configurazione del firewall host

2. Selezionare un nome e l'azione predefinita. In questo caso, selezionare Consenti. 

   Nome configurazione firewall host e azione predefinita

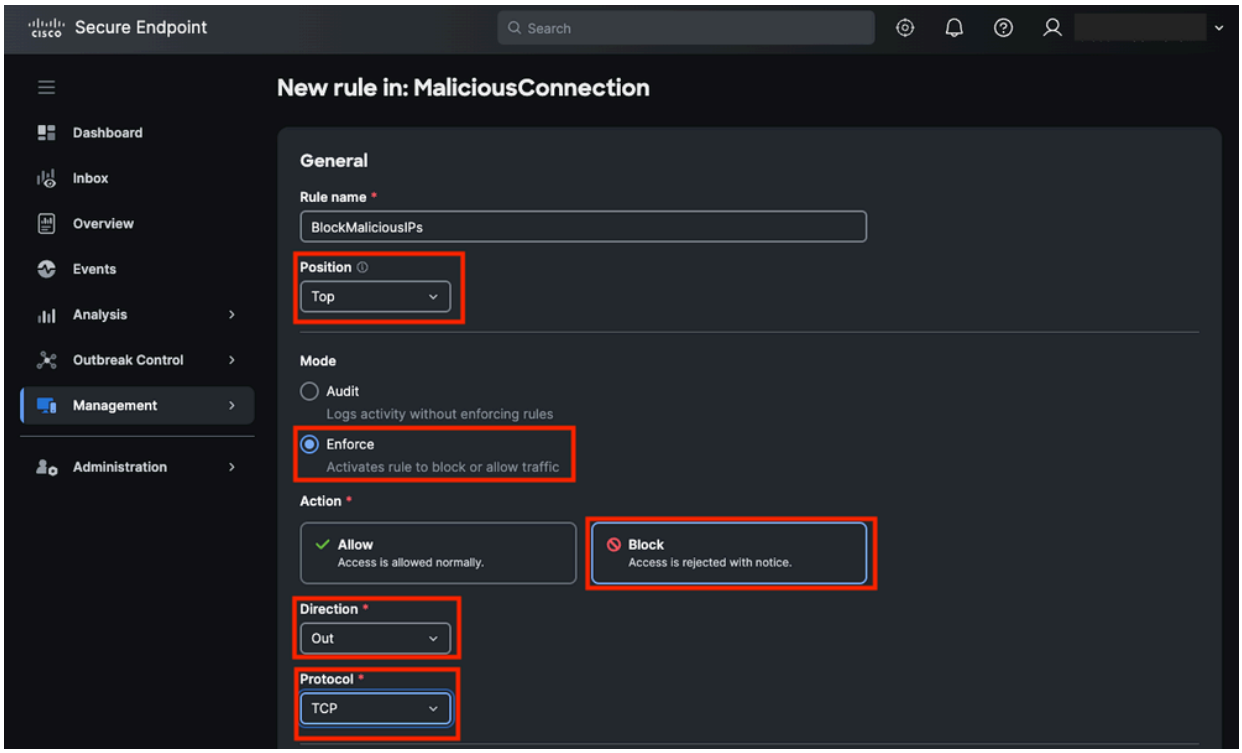


Nota: È necessario creare una regola di blocco, ma è necessario consentire il traffico di altro tipo per evitare l'impatto sulle connessioni legittime.

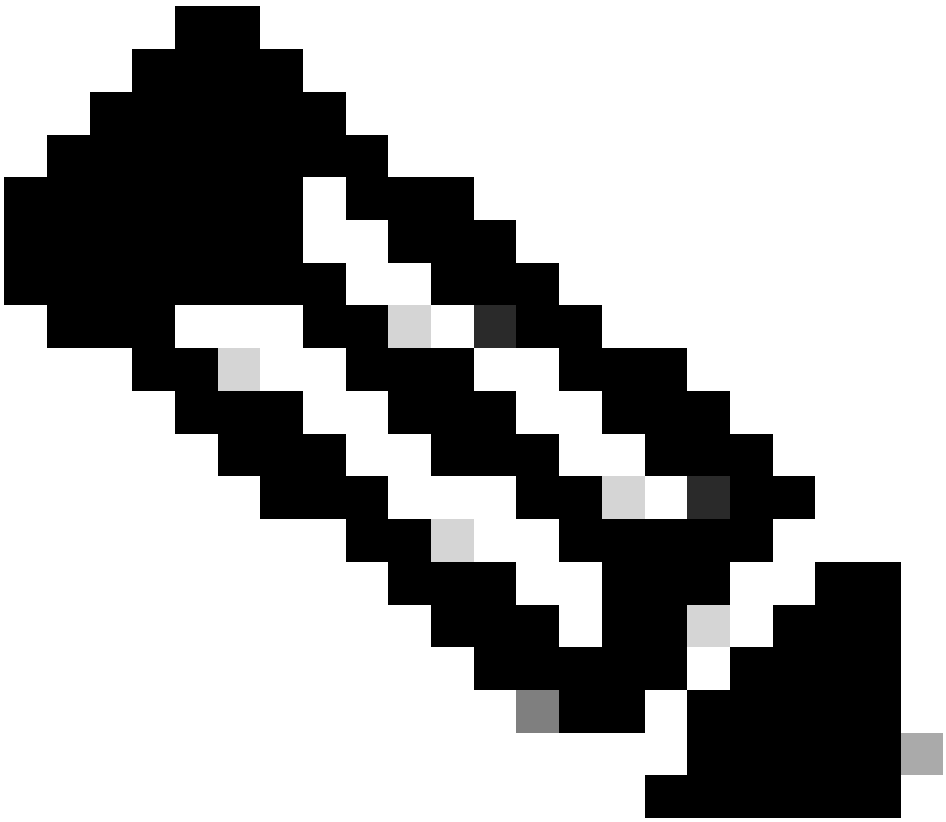
3. Verificare che la regola predefinita sia stata creata e fare clic su Aggiungi regola. 

Aggiungi regola nel firewall host

4. Assegnate un nome e impostate i parametri successivi:
   - Posizione: In alto
   - Modalità: Imponi
   - Azione: Block (Blocca)
   - Direzione: Uscita
   - Protocollo: TCP



Parametri generali regola



Nota: Quando si indirizzano connessioni dannose da un endpoint interno a una destinazione esterna, in genere a Internet, la direzione può sempre essere Fuori.

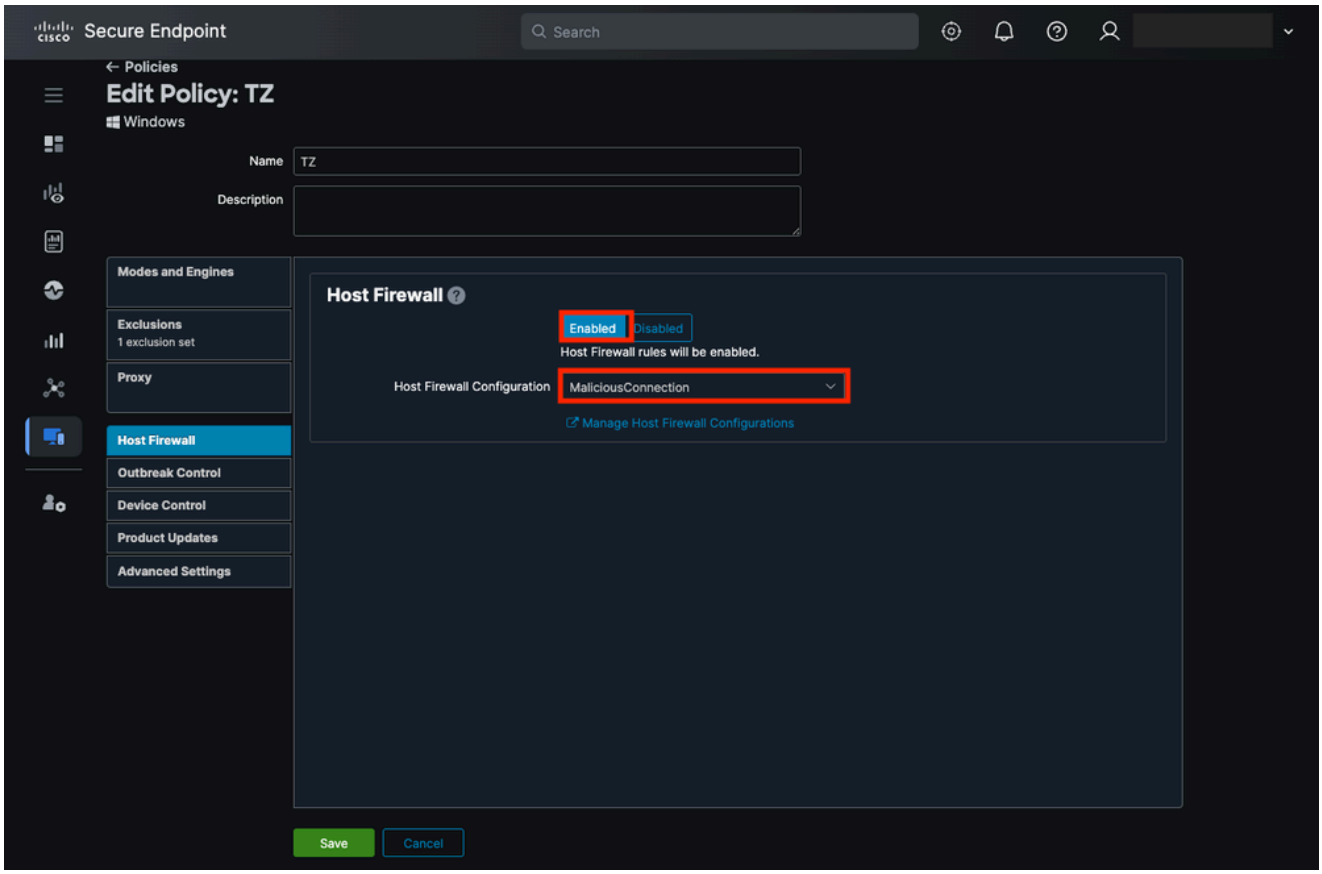
5. Specificare gli IP locale e di destinazione:
    - IP locale: 192.168.0.61
    - IP remoto: 208.94.116.246
    - Lasciare vuoto il campo Portfield locale.
    - Impostare la porta di destinazione su 80 e 443, che corrispondono a HTTP e HTTPS.

    Indirizzi e porte regola

6. Infine, fare clic su Salva.

Abilitare il firewall host nel criterio e assegnare la nuova configurazione

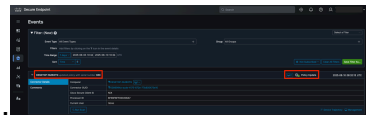
1. Nel portale degli endpoint sicuri, passare a Gestione > Criteri e selezionare il criterio associato all'endpoint in cui si desidera bloccare le attività dannose.
2. Fare clic su Modifica e passare alla scheda Firewall host.
3. Abilitare la funzionalità Host Firewall e selezionare la configurazione recente, in questo caso MaliciousConnection.



Firewall host abilitato nei criteri per gli endpoint sicuri

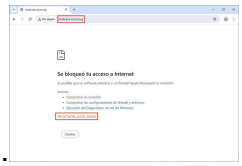
4. Fare clic su Save (Salva).

5. Verificare infine che l'endpoint abbia applicato le modifiche ai criteri.



Evento di aggiornamento criteri

Convalida della configurazione localmente



1. Usare l'URL malware.eicar.org in un browser per confermare che è bloccato.

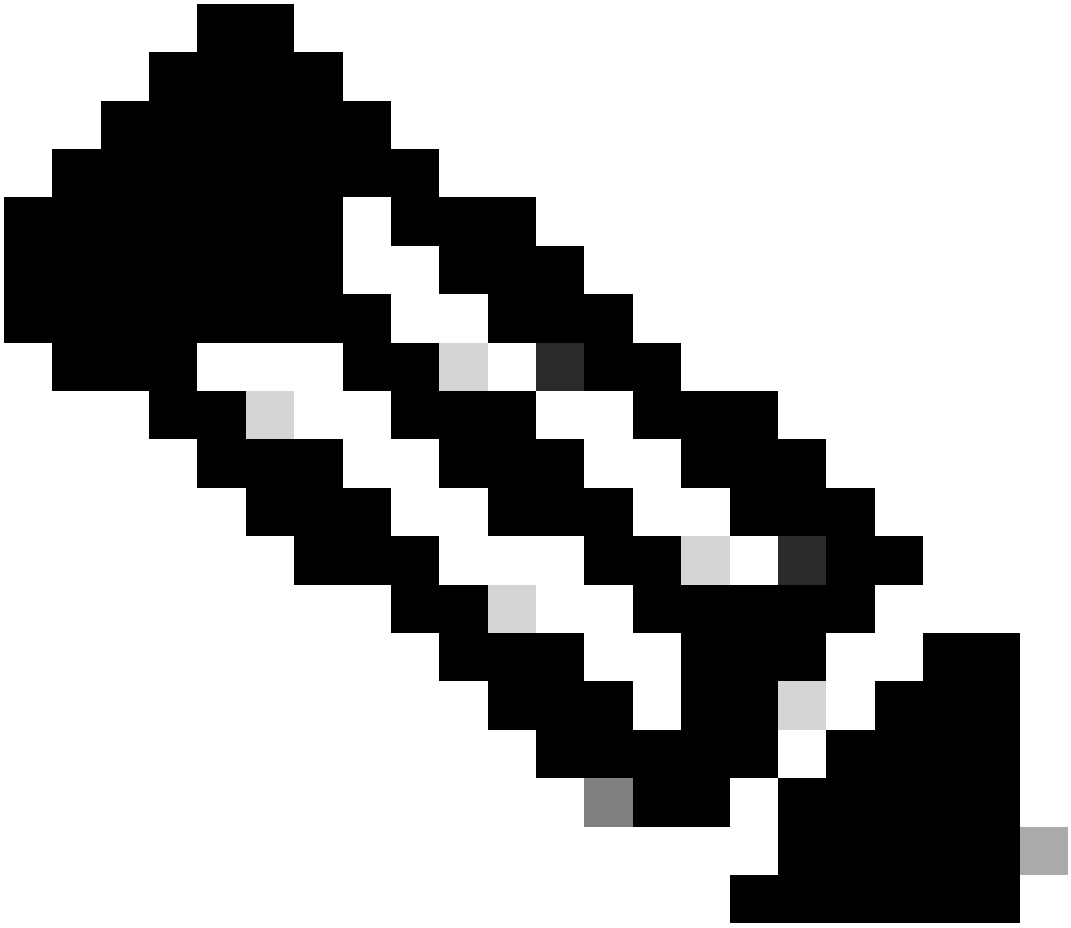
Errore Accesso alla rete negato dal browser

2. Dopo aver confermato il blocco, verificare che non siano state stabilite connessioni. Utilizzare il comando netstat -ano | findstr STABILITO per garantire che l'indirizzo IP associato all'URL dannoso (208.94.116.246) non sia visibile.

Verifica log

1. Sull'endpoint, passare alla cartella:

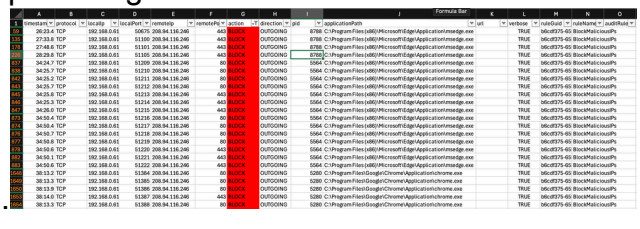
C:\Program Files\Cisco\AMP\<Versione connettore>\FirewallLog.csv



Nota: Il file di registro si trova nella cartella <directory di installazione>\Cisco\AMP\<versione connettore>\FirewallLog.csv

---

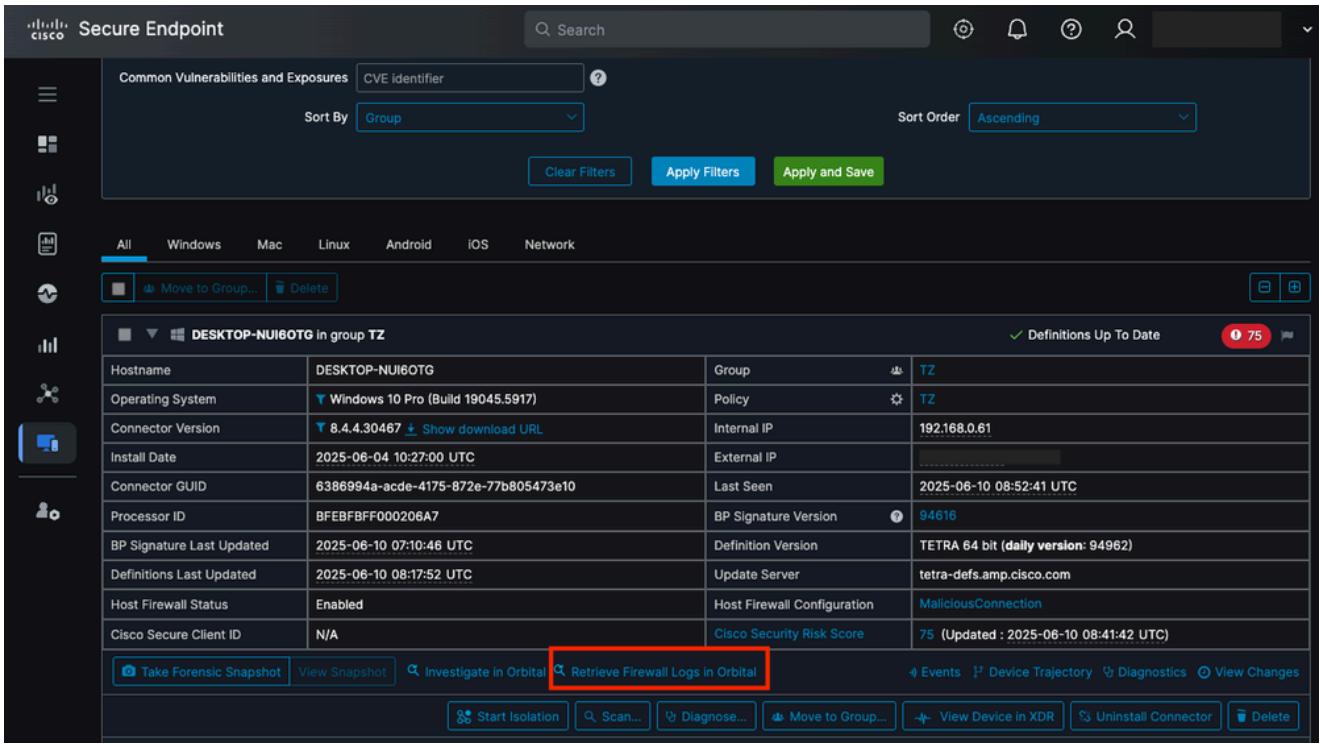
2. Aprire il file CSV per convalidare le corrispondenze per la regola di azione Blocca. Utilizzare un filtro per distinguere le connessioni Consenti e Blocca.



Registri firewall in file CSV

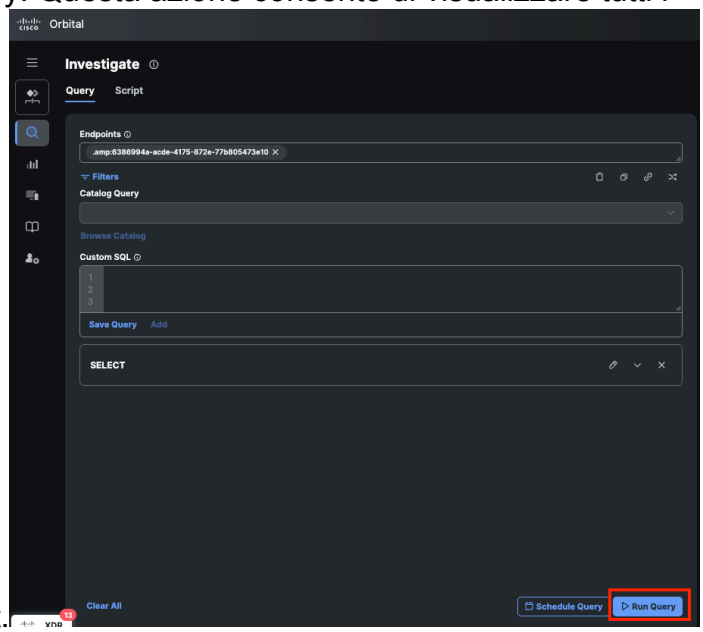
Utilizzare Orbital per recuperare i log del firewall

1. Nel portale degli endpoint sicuri, passare a Gestione > Computer, individuare l'endpoint e fare clic su Recupera log firewall in orbitale. Questa azione reindirizza l'utente al portale orbitale.



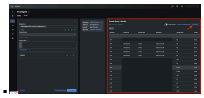
Pulsante per il recupero dei log del firewall in orbitale

2. Nel portale orbitale, fare clic su Esegui query. Questa azione consente di visualizzare tutti i log registrati sull'endpoint per il firewall host.



Esegui query da orbitale

3. Le informazioni sono visibili nella scheda Risultati oppure è possibile scaricarle.



Risultati query da orbitale

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).