Troubleshoot Malicious Connection with Host Firewall

Contents

Introduction

This document describes how to detect malicious connections on a Windows endpoint and block them using the Host Firewall in Cisco Secure Endpoint.

Prerequisites

Requirements

- Host Firewall is available with Secure Endpoint Advantage and Premier packages.
- Supported Connector Versions
  - Windows (x64): Secure Endpoint Windows connector 8.4.2 and later.
  - Windows (ARM): Secure Endpoint Windows connector 8.4.4 and later.

Components Used

This document is not restricted to specific software and hardware versions.

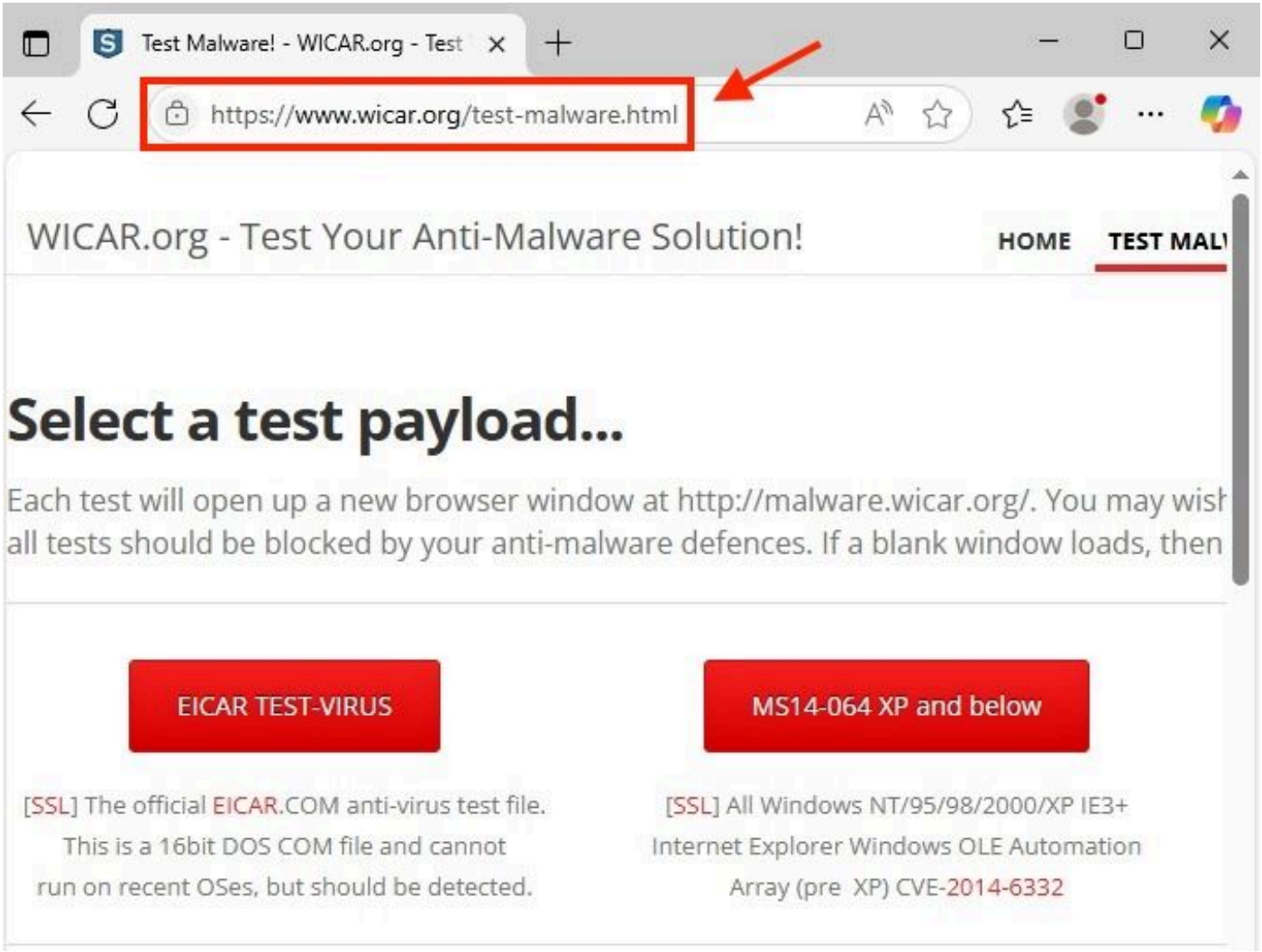
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot Guide

This document provides a guide to block malicious connections with the use of Cisco Secure Endpoint Host Firewall. In order to test, you use the test page malware.wicar.org (208.94.116.246) to create a troubleshoot guide.

Steps to Identify and Block Malicious Connections

1. First, you need to identify the URL or IP address you want to review and block. For this scenario consider malware.wicar.org.
2. Verify if access to the URL is successful. malware.wicar.org redirects to a different URL, as show in the image.



Browser Malicious URL

3. Use the **nslookup** command to retrieve the IP address associated with the 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
```

nslookup Output

4. Once the malicious IP address is obtained, check the **active connections** on the endpoint with the command:**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 for all Connections

5. In order to isolate active connections, apply a **filter** to display only established connections.

```
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 for Established Connections

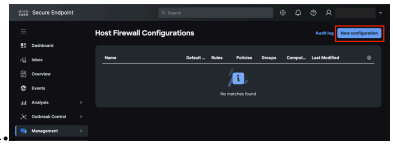
6. Look for the IP address obtained from the**nslookup**command in the previous output. Identify the source IP, destination IP, source port, and destination port.

- **Local IP**: 192.168.0.61
- **Remote IP**: 208.94.116.246
- **Local Port:** Not Applicable
- **Destination Port**to 80 and 443

7. Once you have this information, navigate to the **Cisco Secure Endpoint Portal** to create the **Host Firewall configuration**.

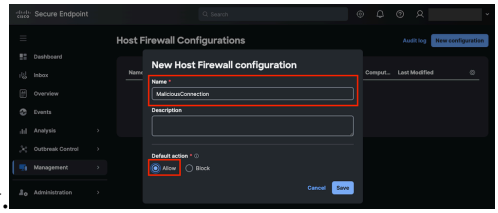
Host Firewall Configuration and Rule Creation

1. Navigate to**Management > Host Firewall**and click**New Configuration**.

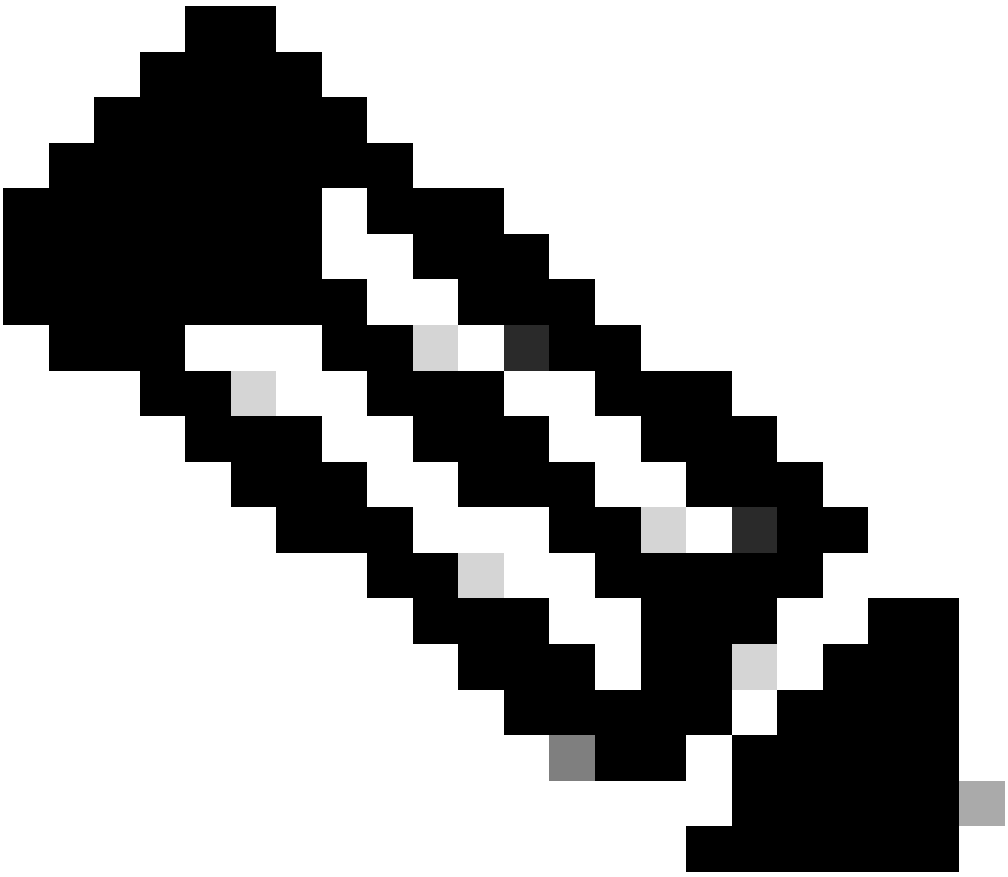


Host Firewall New Configuration

2. Select a **name** and the**Default Action**. In this case, select **Allow**.

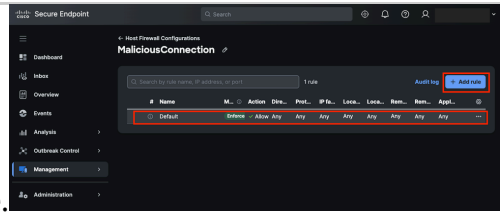


Host Firewall Configuration Name and Default Action



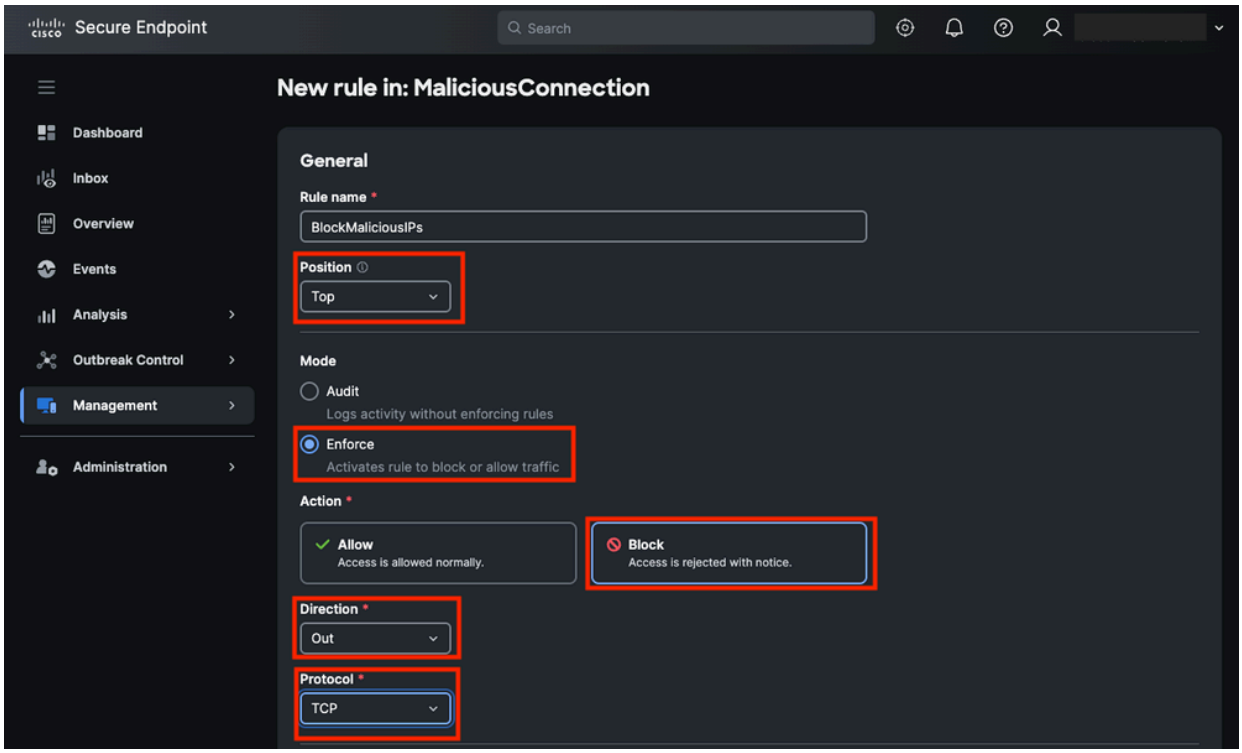
Note: Keep in mind that you create a block rule, but you must allow other traffic to avoid impact on legitimate connections.

3. Verify that the default rule has been created and click**Add Rule**.

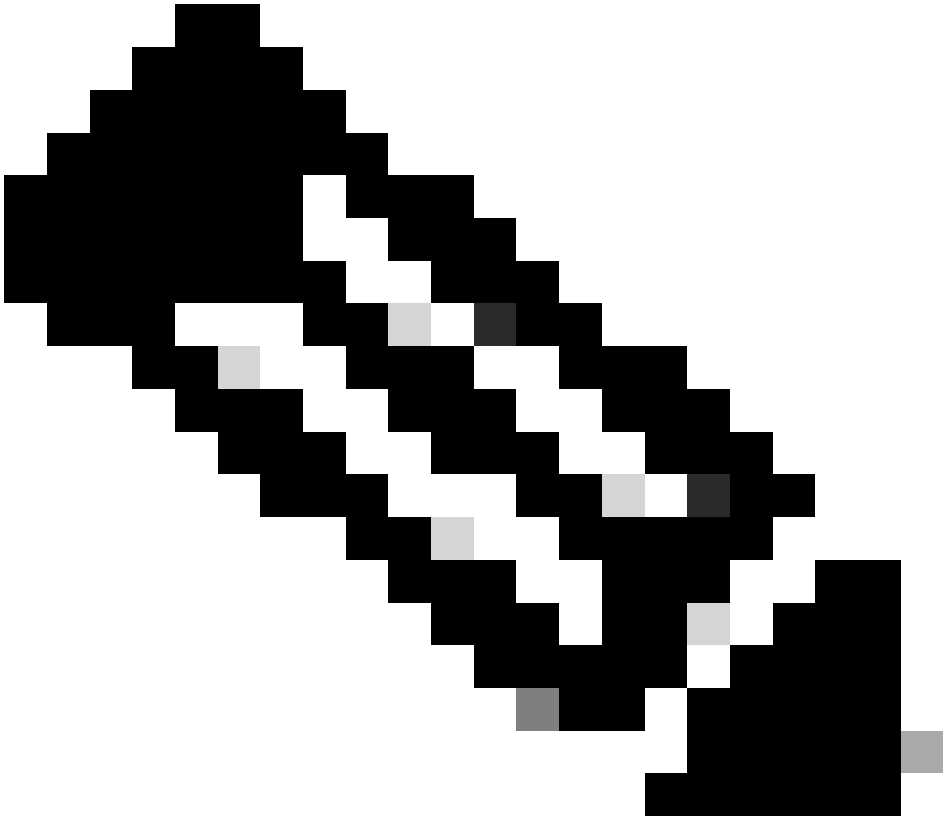


Add Rule in Host Firewall

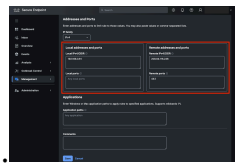
4. Assign a name and set the next parameters:
    - **Position**: Top
    - **Mode**: Enforce
    - **Action**: Block
    - **Direction**: Out
    - **Protocol**: TCP



Rule General Parameters



Note: When you address malicious connections from an internal endpoint to an external destination, typically to the internet, the direction can always be Out.

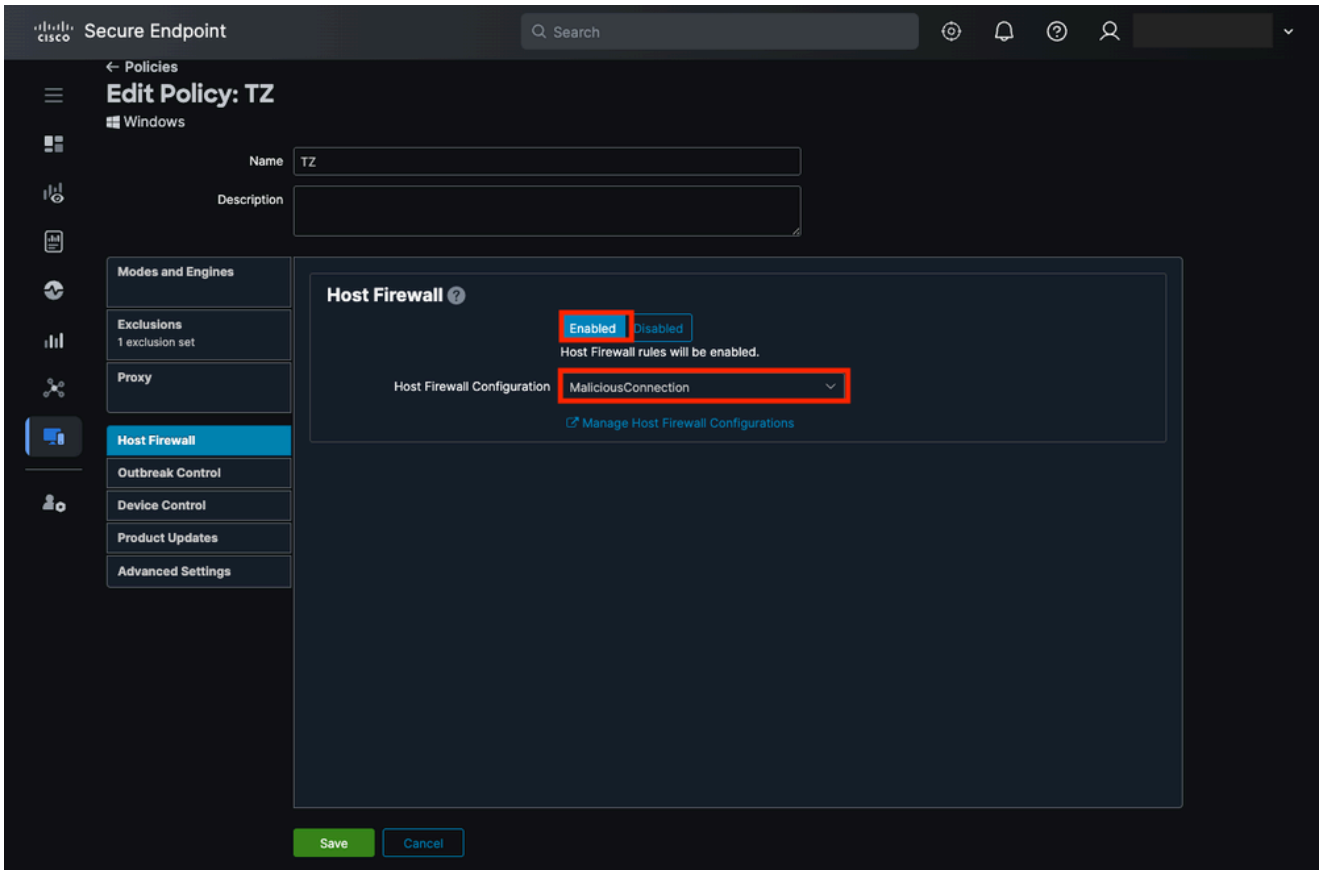
5. Specify the local and destination IPs:
   - **Local IP**: 192.168.0.61
   - **Remote IP**: 208.94.116.246
   - Leave the**Local Port**field blank.
   - Set the**Destination Port**to 80 and 443, these correspond to HTTP and HTTPS. 

     Rule Addresses and Ports

6. Finally, click**Save**.

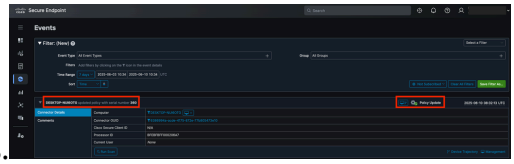
Enable Host Firewall in the Policy and Assign the New Configuration

1. In the Secure Endpoint Portal, navigate to**Management > Policies**and select the **policy** associated with the endpoint where you want to block malicious activity.
2. Click**Edit**and navigate to the**Host Firewall**tab.
3. Enable the **Host Firewall** feature and select the recent configuration, in this case **MaliciousConnection.**



Host Firewall Enabled in Secure Endpoint Policy

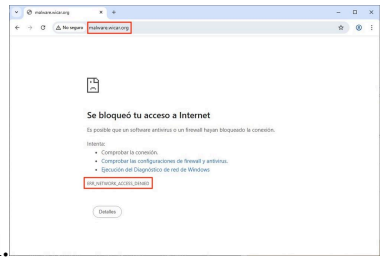
4. Click **Save**.



5. Finally, verify that the endpoint has applied the policy changes.

Policy Update Event

Validate the Configuration Locally



1. Use the URL malware.eicar.org in a browser to confirm that it is blocked.

Error Network Access Denied from Browser

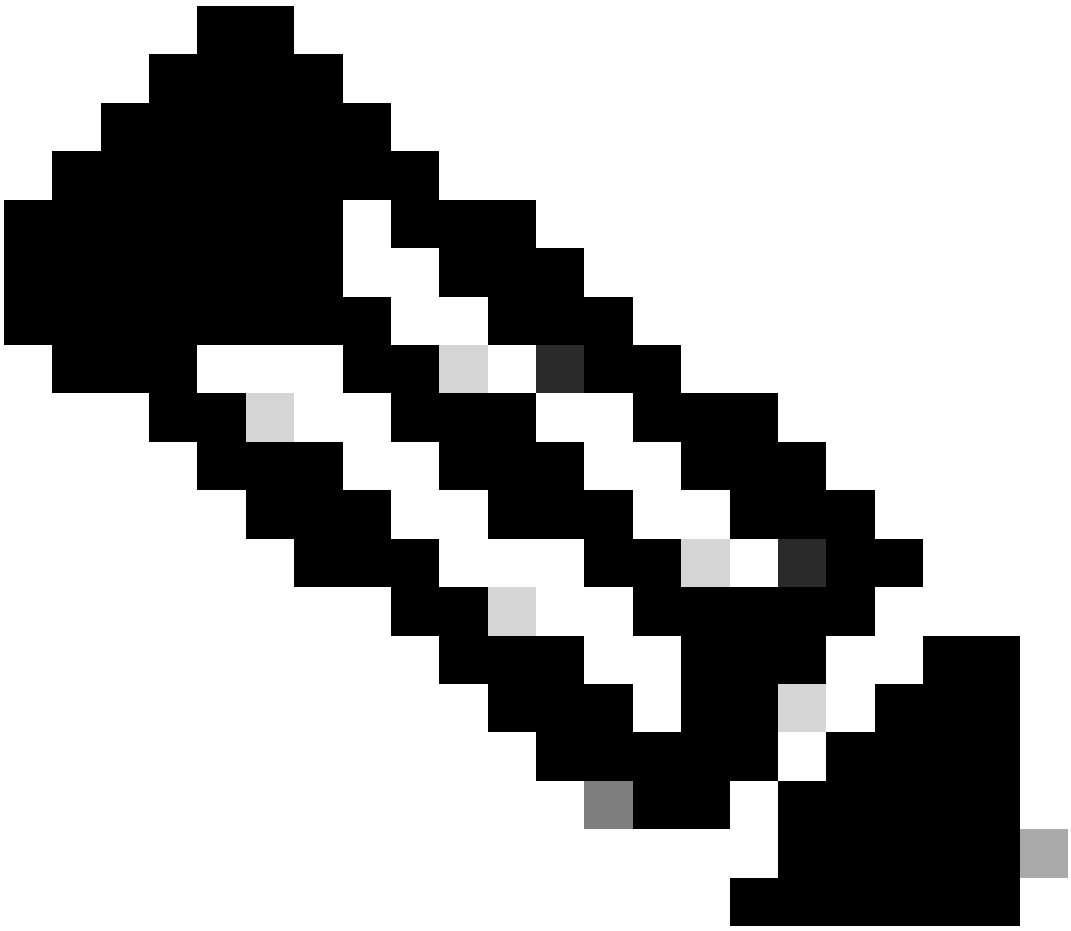
2. After you confirm the block, verify that no connections are established. Use the command **netstat -ano | findstr ESTABLISHED** to ensure the IP associated with the malicious URL (208.94.116.246) is not visible.

Review Logs

1. On the endpoint, navigate to the **folder**:

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

---



Note: The log file is located in the folder <install directory>\Cisco\AMP\<Connector version>\FirewallLog.csv

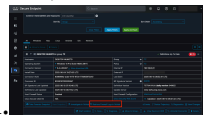
---

2. Open the **CSV file** to validate matches for the Block action rule. Use a filter to distinguish between Allow and Block connections.

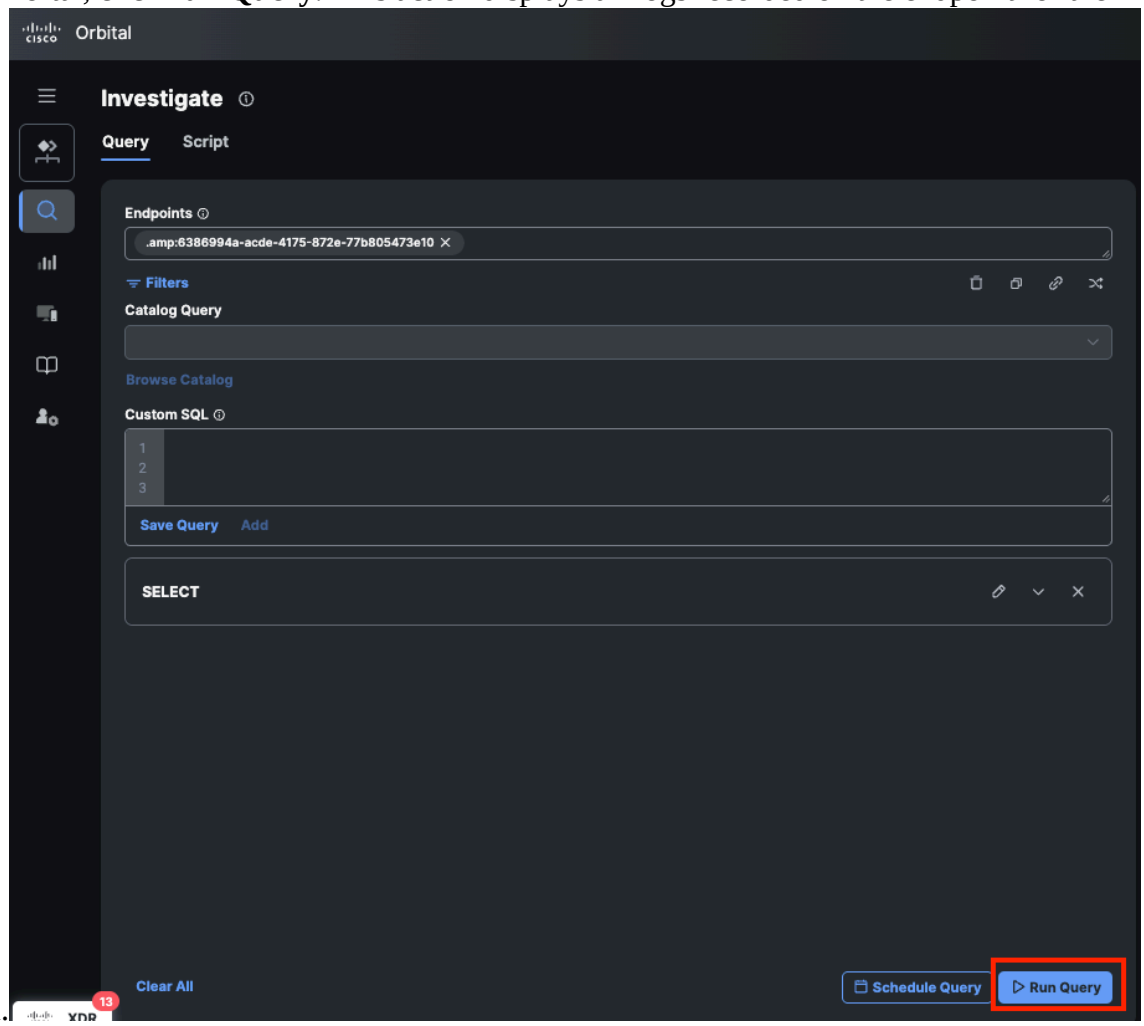
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	timestam	protocol	localIp	localPort	remoteIp	remotePo	action	direction	pid	applicationPath	url	verbose	ruleGuid	ruleName	auditRule
59	26:23.4	TCP	192.168.0.61	50675	208.94.116.246	443	BLOCK	OUTGOING	8788	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
135	27:33.8	TCP	192.168.0.61	51100	208.94.116.246	443	BLOCK	OUTGOING	8788	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
178	27:48.6	TCP	192.168.0.61	51101	208.94.116.246	443	BLOCK	OUTGOING	8788	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
228	28:29.8	TCP	192.168.0.61	51105	208.94.116.246	443	BLOCK	OUTGOING	8788	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
837	34:24.7	TCP	192.168.0.61	51209	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
838	34:25.7	TCP	192.168.0.61	51210	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
842	34:25.2	TCP	192.168.0.61	51211	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
843	34:25.7	TCP	192.168.0.61	51212	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
845	34:25.8	TCP	192.168.0.61	51213	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
846	34:25.3	TCP	192.168.0.61	51214	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
847	34:26.0	TCP	192.168.0.61	51215	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
873	34:50.4	TCP	192.168.0.61	51216	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
874	34:50.4	TCP	192.168.0.61	51217	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
876	34:50.7	TCP	192.168.0.61	51218	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
877	34:50.8	TCP	192.168.0.61	51219	208.94.116.246	80	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
878	34:50.6	TCP	192.168.0.61	51220	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
882	34:50.1	TCP	192.168.0.61	51221	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
883	34:50.6	TCP	192.168.0.61	51222	208.94.116.246	443	BLOCK	OUTGOING	5564	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
1648	38:13.2	TCP	192.168.0.61	51384	208.94.116.246	80	BLOCK	OUTGOING	5280	C:\Program Files\Google\Chrome\Application\chrome.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
1649	38:13.3	TCP	192.168.0.61	51385	208.94.116.246	80	BLOCK	OUTGOING	5280	C:\Program Files\Google\Chrome\Application\chrome.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
1650	38:13.9	TCP	192.168.0.61	51386	208.94.116.246	80	BLOCK	OUTGOING	5280	C:\Program Files\Google\Chrome\Application\chrome.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
1653	38:14.0	TCP	192.168.0.61	51387	208.94.116.246	443	BLOCK	OUTGOING	5280	C:\Program Files\Google\Chrome\Application\chrome.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	
1654	38:13.3	TCP	192.168.0.61	51388	208.94.116.246	80	BLOCK	OUTGOING	5280	C:\Program Files\Google\Chrome\Application\chrome.exe		TRUE	b6cdf375-65	BlockMaliciousIPs	

Firewall Logs in CSV File

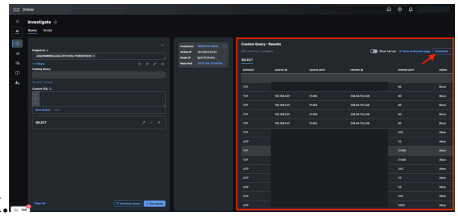
Use Orbital to Retrieve Firewall Logs

1. In the Secure Endpoint Portal, navigate to**Management > Computers**, locate the endpoint, and click**Retrieve Firewall Logs in Orbital**. This action redirects you to the Orbital Portal. 

Button to Retrieve Firewall Logs in Orbital

2. In the Orbital Portal, click**Run Query**. This action displays all logs recorded on the endpoint for the Host Firewall. 

Run Query from Orbital

3. The information is visible in the**Results**tab, or you can download it. 

Query Results from Orbital