Fehlerbehebung bei schädlicher Verbindung mit Host-Firewall

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie schädliche Verbindungen auf einem Windows-Endgerät erkannt und mithilfe der Host-Firewall in Cisco Secure Endpoint blockiert werden können.

Voraussetzungen

Anforderungen

- Die Host-Firewall ist mit Secure Endpoint Advantage- und Premier-Paketen verfügbar.
- Unterstützte Connector-Versionen
  - Windows (x64): Secure Endpoint Windows Connector 8.4.2 und höher.
  - Fenster (ARM): Secure Endpoint Windows Connector 8.4.4 und höher.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

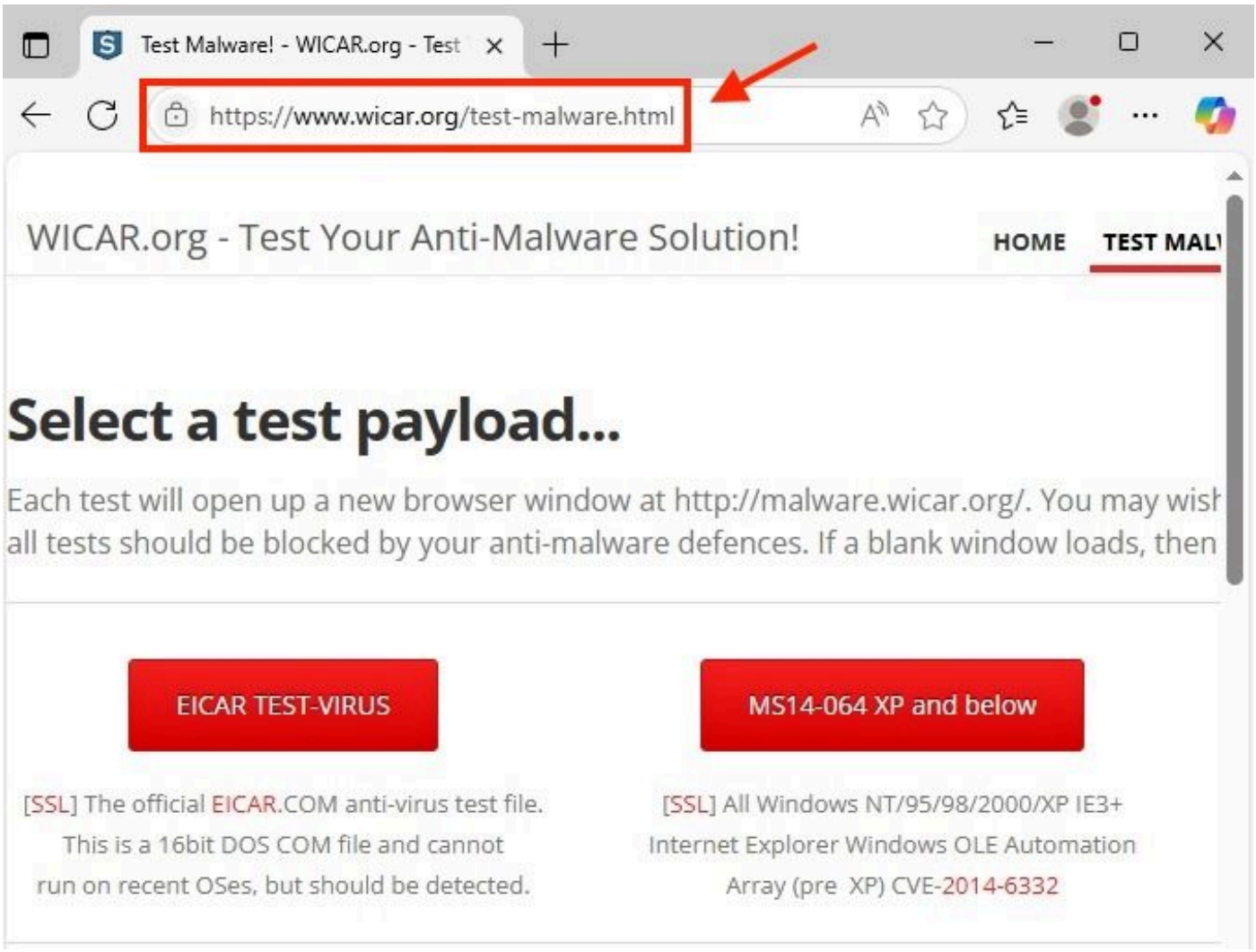
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Leitfaden zur Fehlerbehebung

Dieses Dokument enthält einen Leitfaden zur Blockierung schädlicher Verbindungen mithilfe der Cisco Secure Endpoint Host Firewall. Verwenden Sie zum Testen die Testseite malware.wicar.org (208.94.116.246), um eine Anleitung zur Fehlerbehebung zu erstellen.

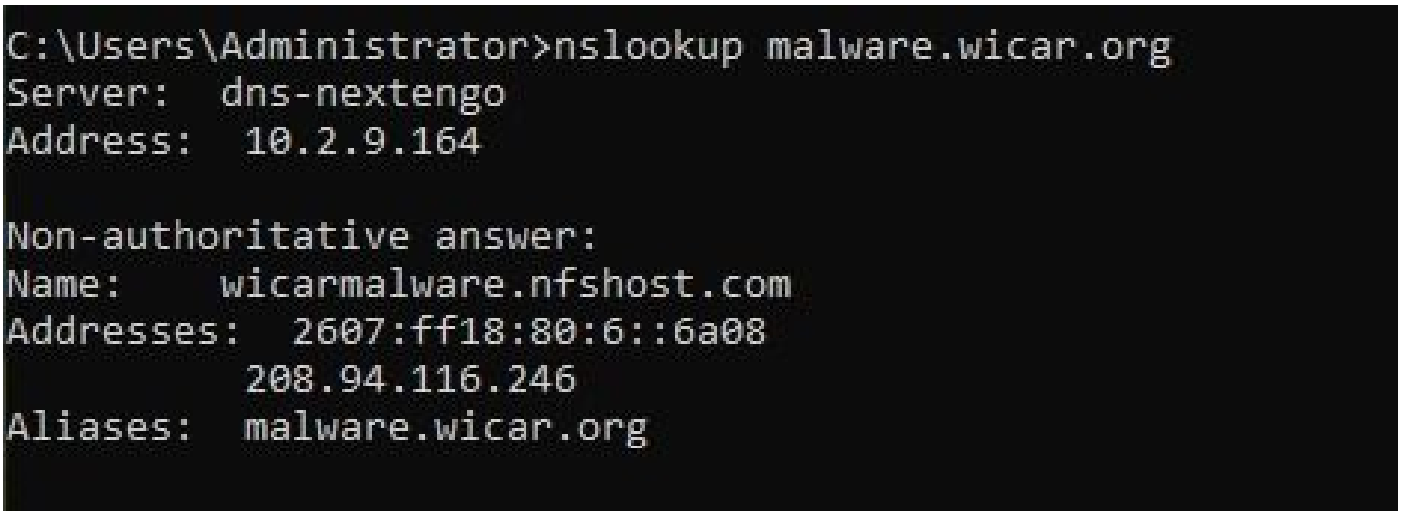
Schritte zur Identifizierung und Blockierung schädlicher Verbindungen

1. Zuerst müssen Sie die URL oder die IP-Adresse angeben, die Sie überprüfen und blockieren möchten. Für dieses Szenario consider malware.wicar.org.
2. Überprüfen Sie, ob der Zugriff auf die URL successful. malware.wicar.org zu einer anderen URL umleitet, wie im Bild gezeigt.



Schädliche URL im Browser

3. Verwenden Sie den Befehl nslookup, um die IP-Adresse abzurufen, die der URL malware.wicar.org zugeordnet ist.



nslookup-Ausgabe

4. Sobald die schädliche IP-Adresse abgerufen wurde, überprüfen Sie die aktiven Verbindungen auf dem Endpunkt mit dem Befehl: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 für alle Verbindungen

5. Um aktive Verbindungen zu isolieren, wenden Sie einen Filter an, um nur bestehende Verbindungen anzuzeigen.

```
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 für etablierte Verbindungen

6. Suchen Sie in der vorherigen Ausgabe nach der IP-Adresse, die aus dem BefehlLookUp abgerufen wurde. Geben Sie die Quell-IP, die Ziel-IP, den Quell-Port und den Ziel-Port an.

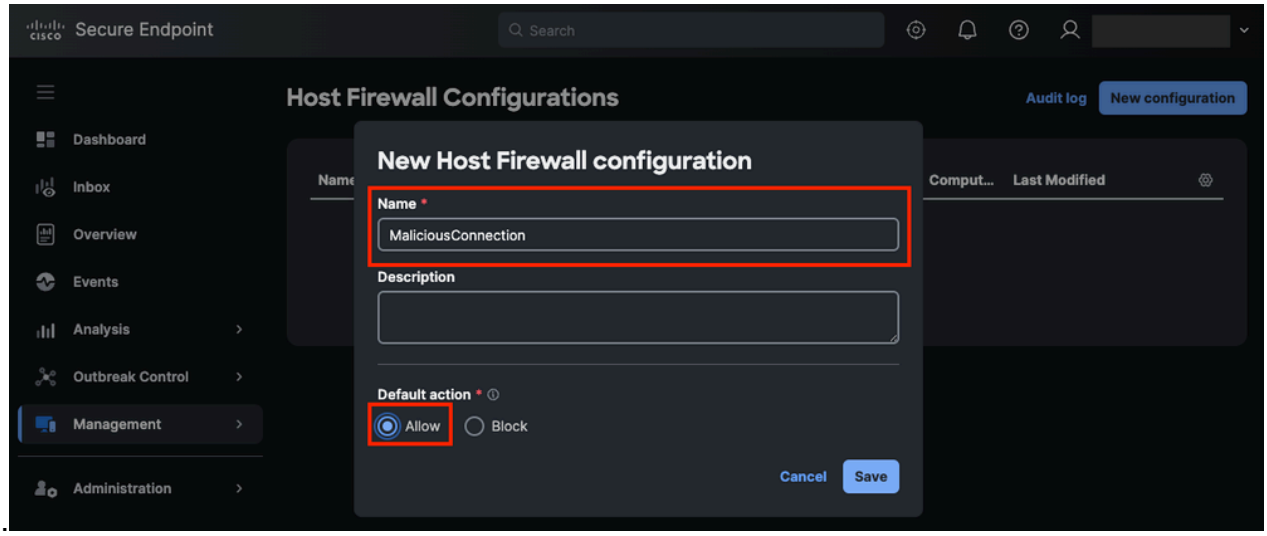
- Lokale IP: 192.168.0.61
- Remote-IP: 208.94.116.246
- Lokaler Port: Nicht zutreffend
- Zielportto 80 und 443

7. Sobald Sie über diese Informationen verfügen, navigieren Sie zum Cisco Secure Endpoint Portal, um die Host-Firewall-Konfiguration zu erstellen.

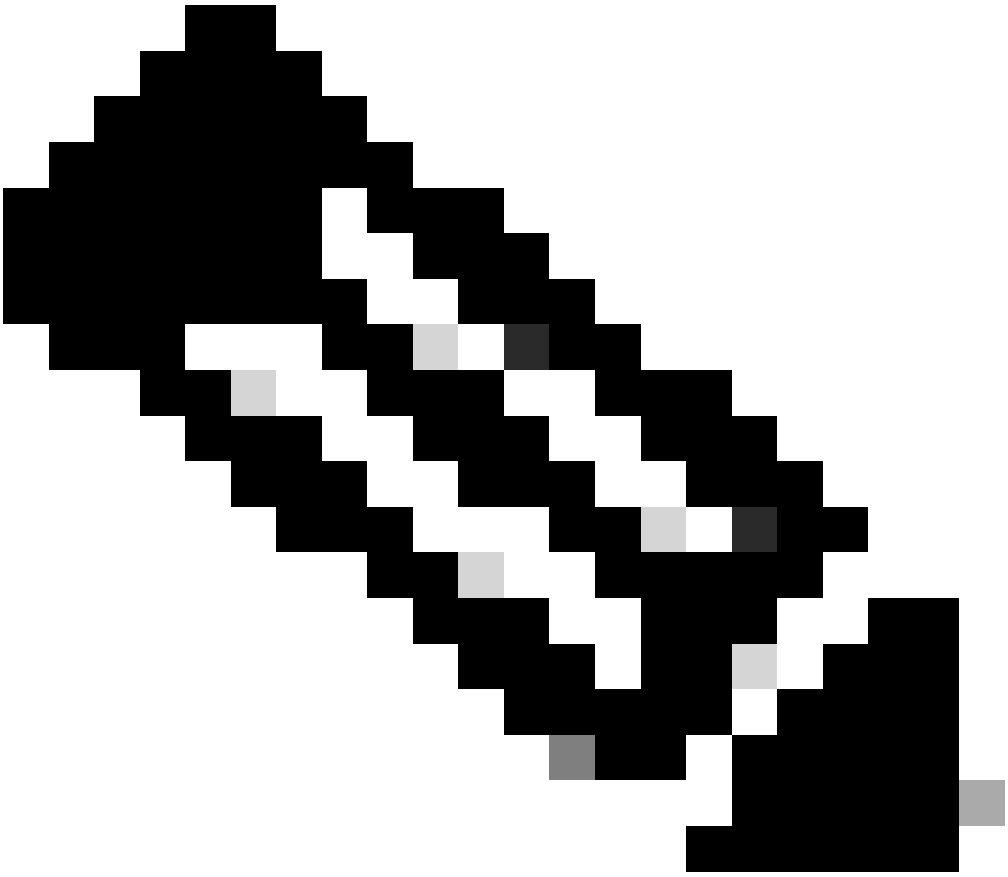
Host-Firewall-Konfiguration und Regelerstellung

1. Navigieren Sie zuManagement > Host Firewall, und klicken Sie auf New Configuration. 

   Neue Host-Firewall-Konfiguration

2. Wählen Sie einen Namen und die Standardaktion aus. Wählen Sie in diesem Fall Zulassen aus. 

Konfigurationsname und Standardaktion der Host-Firewall

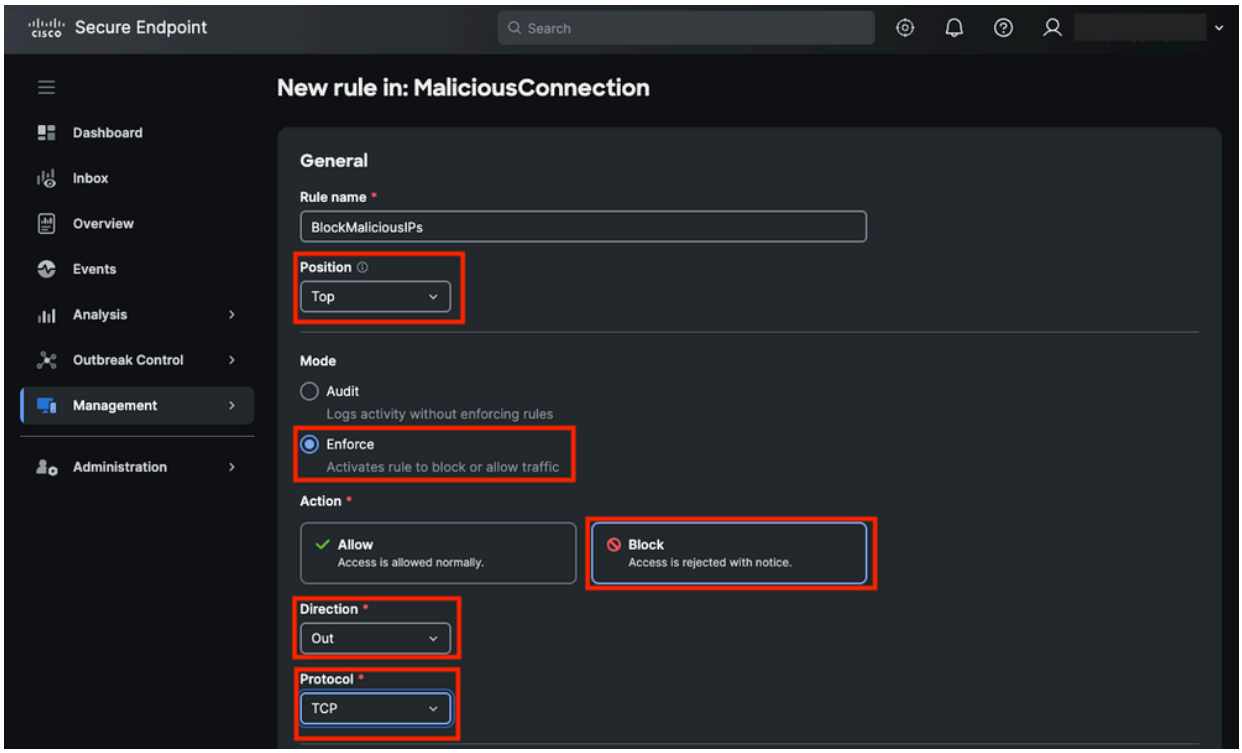


Anmerkung: Beachten Sie, dass Sie eine Blockregel erstellen, Sie müssen jedoch anderen Datenverkehr zulassen, um Auswirkungen auf legitime Verbindungen zu vermeiden.

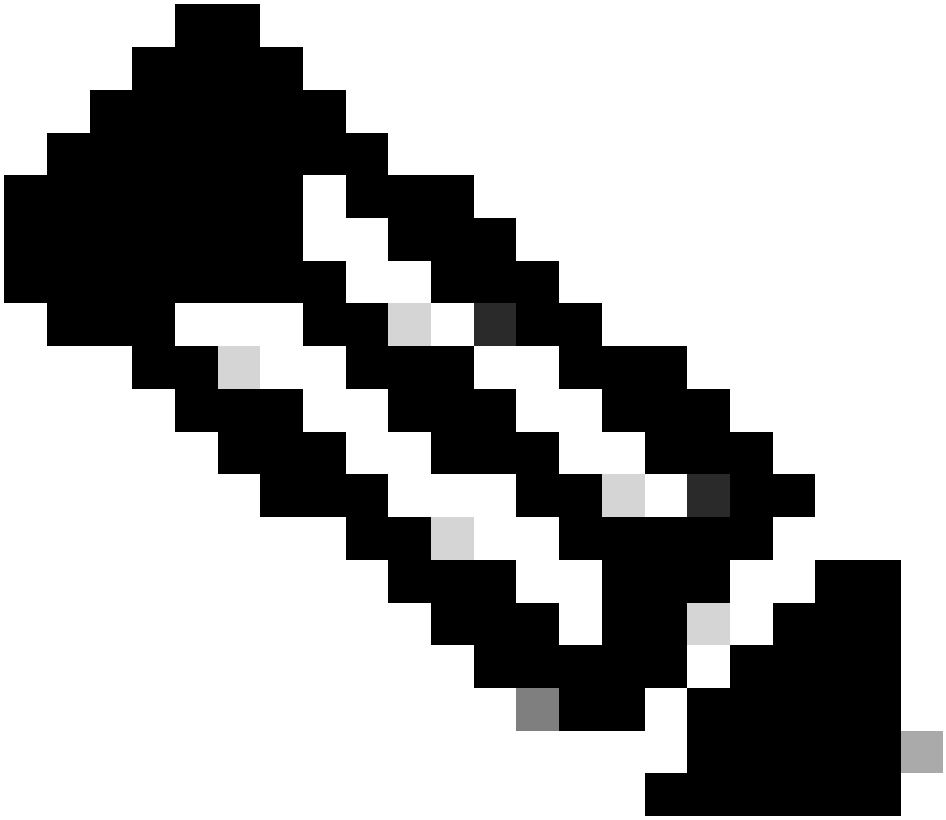
3. Überprüfen Sie, ob die Standardregel erstellt wurde, und klicken Sie auf Regel hinzufügen.

Regel in Host-Firewall hinzufügen

4. Weisen Sie einen Namen zu, und legen Sie die nächsten Parameter fest:
   - Position: Oben
   - Modus: Durchsetzen
   - Aktion: Blockieren
   - Richtung: Aus
   - Protokolle: TCP



Allgemeine Parameter der Regel



Anmerkung: Wenn Sie schädliche Verbindungen von einem internen Endpunkt zu einem externen Ziel, in der Regel zum Internet, bekämpfen, kann die Richtung immer Out sein.

5. Geben Sie die lokalen IPs und die Ziel-IPs an:
   - Lokale IP: 192.168.0.61
   - Remote-IP: 208.94.116.246
   - Lassen Sie das Feld "Lokaler Port" leer.
   - Legen Sie den Zielport auf 80 und 443 fest. Diese entsprechen HTTP und HTTPS. 

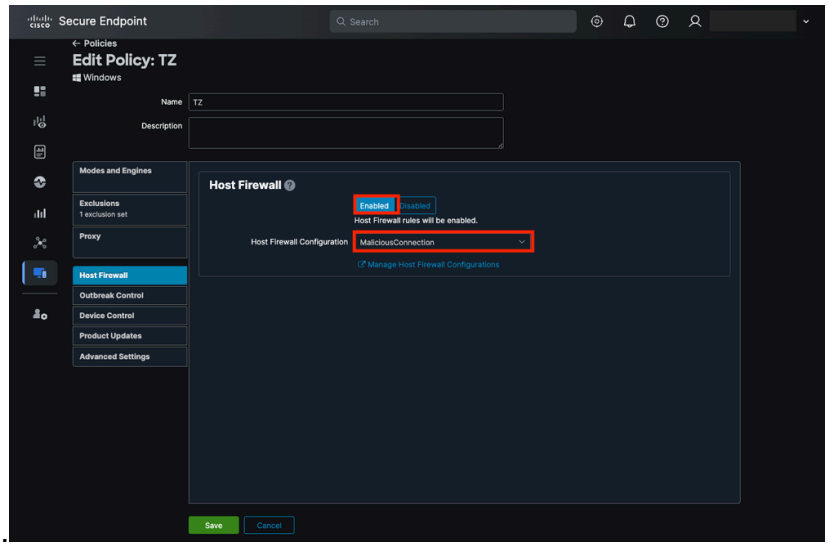
     Regeladressen und -ports

6. Schließlich klicken Sie auf Speichern.

Aktivieren der Host-Firewall in der Richtlinie und Zuweisen der neuen Konfiguration

1. Navigieren Sie im sicheren Endgeräteportal zuManagement > Policies (Verwaltung > Richtlinien), und wählen Sie die Richtlinie aus, die mit dem Endpunkt verknüpft ist, an dem Sie schädliche Aktivitäten blockieren möchten.
2. Klicken Sie auf Bearbeiten, und navigieren Sie zur Registerkarte Host-Firewall.
3. Aktivieren Sie die Host-Firewall-Funktion, und wählen Sie die aktuelle Konfiguration aus, in

diesem Fall "MaliciousConnection".



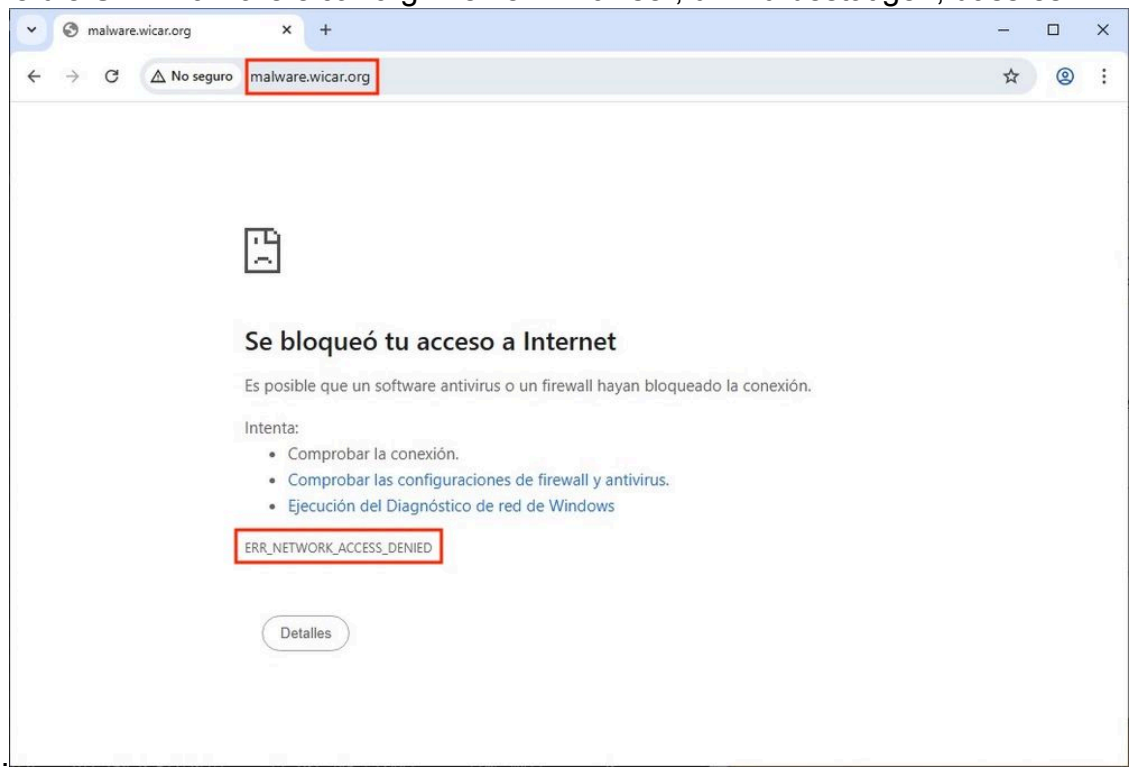
Host-Firewall in Richtlinie für sichere Endgeräte aktiviert

4. Klicken Sie auf Speichern.
5. Überprüfen Sie abschließend, ob der Endpunkt die Richtlinienänderungen angewendet hat.

Ereignis für Richtlinienaktualisierung

Lokale Validierung der Konfiguration

1. Verwenden Sie die URL malware.eicar.org in einem Browser, um zu bestätigen, dass es blockiert wird.



Fehler: Netzwerkzugriff vom Browser verweigert

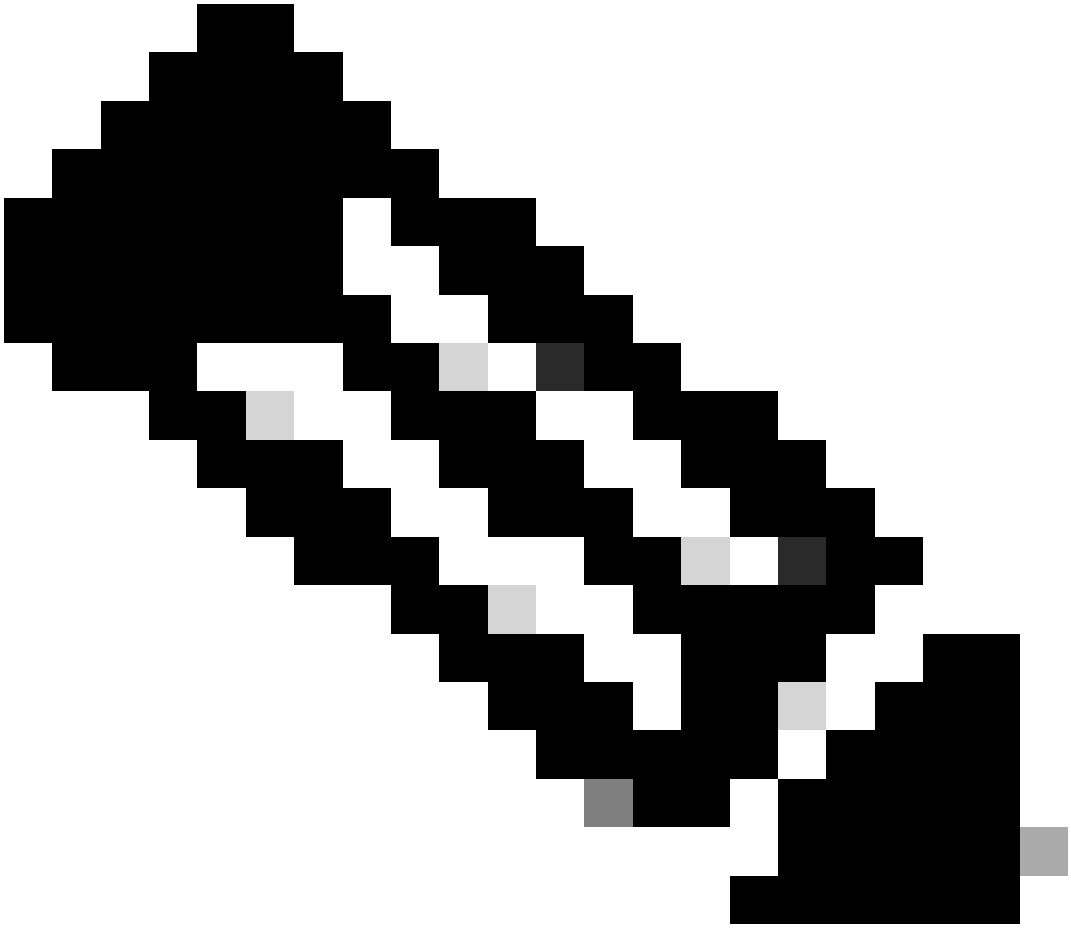
2. Nachdem Sie die Sperre bestätigt haben, stellen Sie sicher, dass keine Verbindungen hergestellt wurden. Verwenden Sie den Befehl netstat -ano | findstr EINGERICHTET, um sicherzustellen, dass die mit der schädlichen URL (208.94.116.246) verknüpfte IP nicht sichtbar ist.

Protokolle überprüfen

1. Navigieren Sie auf dem Endpunkt zum Ordner:

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

---



Anmerkung: Die Protokolldatei befindet sich im Ordner <Installationsverzeichnis>\Cisco\AMP\<Connector-Version>\FirewallLog.csv

---

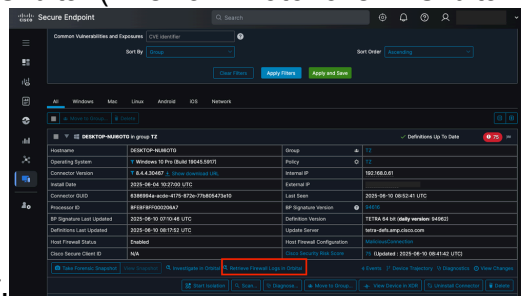
2. Öffnen Sie die CSV-Datei, um Übereinstimmungen für die Sperraktionsregel zu überprüfen. Verwenden Sie einen Filter, um zwischen Zulassen und Sperren von Verbindungen zu unterscheiden.

	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	
226	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-Protokolle in CSV-Datei

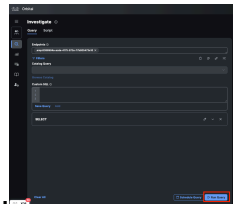
Orbital zum Abrufen von Firewall-Protokollen verwenden

1. Navigieren Sie im Secure Endpoint Portal zuManagement > Computers, suchen Sie den Endpunkt, und klicken Sie auf Retrieve Firewall Logs in Orbital (Firewall-Protokolle in Orbital abrufen). Diese Aktion leitet Sie zum Orbitalportal weiter.



Schaltfläche zum Abrufen von Firewall-Protokollen im Orbit

2. Klicken Sie im Orbitalportal auf Abfrage ausführen. Mit dieser Aktion werden alle Protokolle angezeigt, die auf dem Endpunkt für die Host-Firewall aufgezeichnet wurden.



Abfrage von Orbital ausführen

3. Die Informationen sind in der Ergebnistabelle sichtbar, oder Sie können sie herunterladen.

Abfrageergebnisse aus Orbital

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.