호스트 방화벽으로 악의적인 연결 문제 해결

목차

소개

이 문서에서는 Windows 엔드포인트에서 악의적인 연결을 탐지하고 Cisco Secure Endpoint의 호스트 방화벽을 사용하여 이를 차단하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- 호스트 방화벽은 Secure Endpoint Advantage 및 Premier 패키지와 함께 사용할 수 있습니다.
- 지원되는 커넥터 버전
  - Windows(x64): 보안 엔드포인트 Windows 커넥터 8.4.2 이상
  - Windows(ARM): 보안 엔드포인트 Windows 커넥터 8.4.4 이상

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

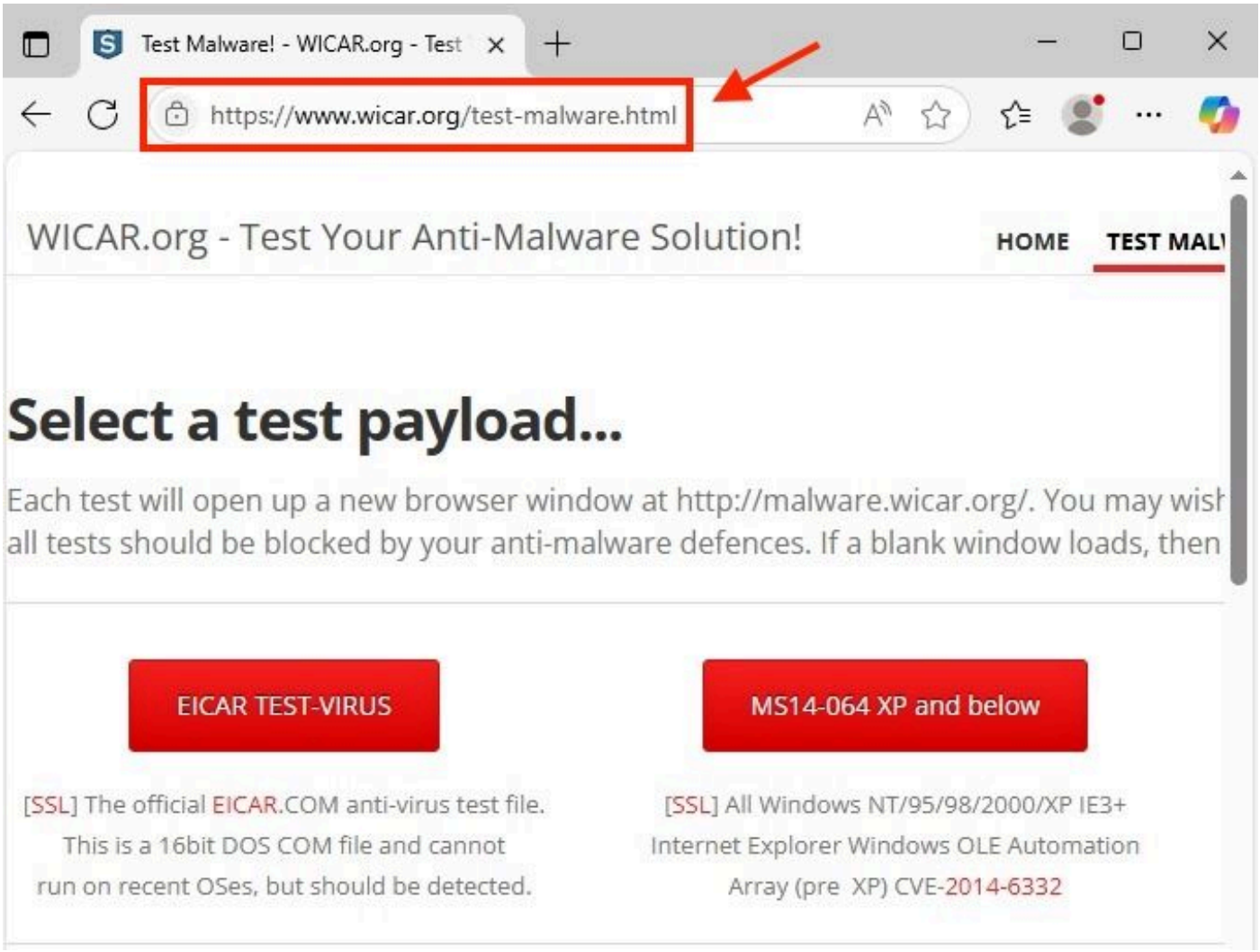
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제 해결 가이드

이 문서에서는 Cisco Secure Endpoint Host Firewall을 사용하여 악의적인 연결을 차단하는 방법을 설명합니다. 테스트하려면 테스트 페이지 malware.wicar.org(208.94.116.246)을 사용하여 문제 해결 가이드를 만듭니다.

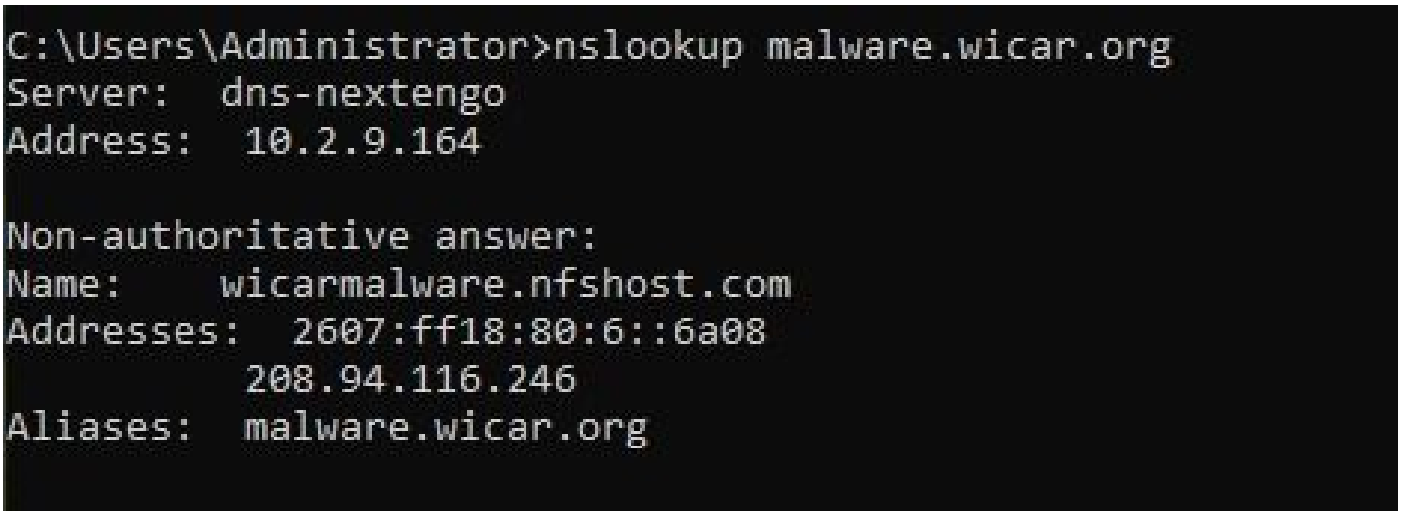
악성 연결을 식별하고 차단하는 단계

1. 먼저 검토하고 차단할 URL 또는 IP 주소를 식별해야 합니다. 이 시나리오의 경우 consider malware.wicar.org을 참조하십시오.
2. 이미지에 표시된 대로 URL에 대한 액세스가 successful. malware.wicar.org인지 확인하고 다른 URL로 리디렉션합니다.



브라우저 악성 URL

3. nslookup 명령을 사용하여 URL malware.wicar.org과 연결된 IP 주소를 검색합니다.



nslookup 출력

4. 악의적인 IP 주소를 얻은 후에는 netstat -ano 명령을 사용하여 엔드포인트의 활성 연결을 확인합니다.

```
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
```

모든 연결에 대한 netstat

5. 활성 연결을 격리하려면 필터를 적용하여 설정된 연결만 표시합니다.

```
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>
```

설정된 연결에 대한 netstat

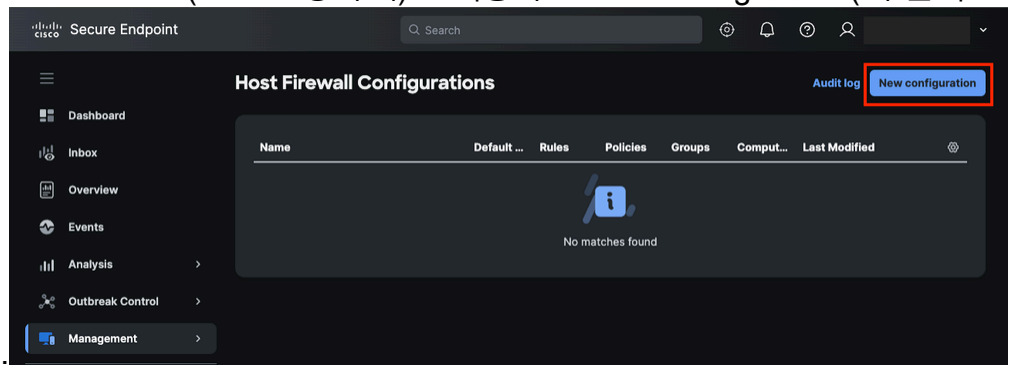
6. 이전 출력의 slookupcommand에서 얻은 IP 주소를 확인합니다. 소스 IP, 목적지 IP, 소스 포트 및 목적지 포트를 식별합니다.

- 로컬 IP: 192.168.0.61
- 원격 IP: 208.94.116.246
- 로컬 포트: 해당 없음
- 대상 포트 80 및 443

7. 이 정보가 있으면 Cisco Secure Endpoint Portal(Cisco Secure Endpoint 포털)로 이동하여 호스트 방화벽 컨피그레이션을 생성합니다.

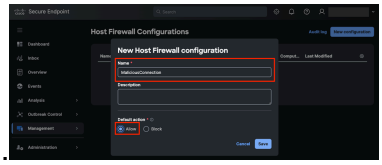
호스트 방화벽 컨피그레이션 및 규칙 생성

1. Management(관리) > Host Firewall(호스트 방화벽)로 이동하고 New Configuration(새 컨피그레이션)을 클릭합니다.

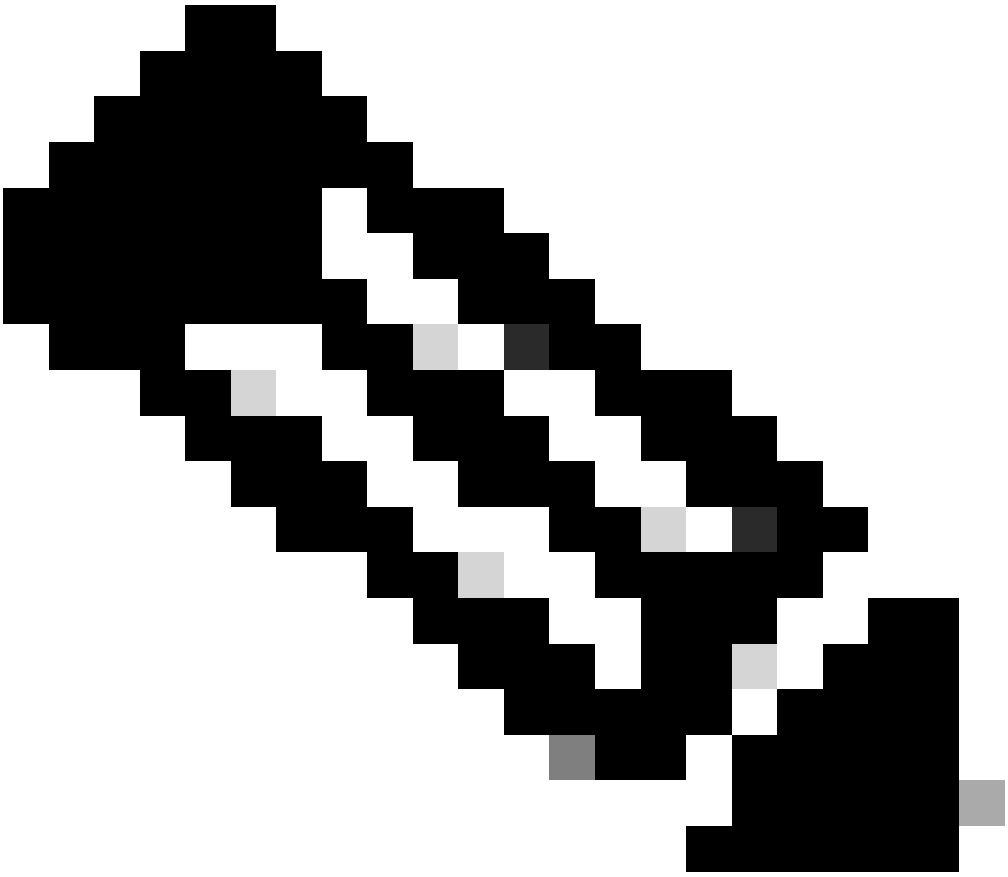


호스트 방화벽 새 컨피그레이션

2. 이름과 기본 작업을 선택합니다. 이 경우 Allow(허용)를 선택합니다.

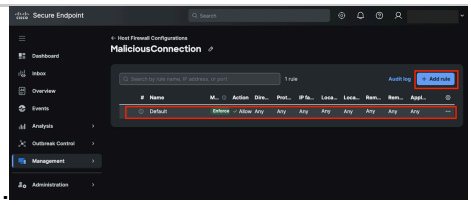


호스트 방화벽 컨피그레이션 이름 및 기본 작업



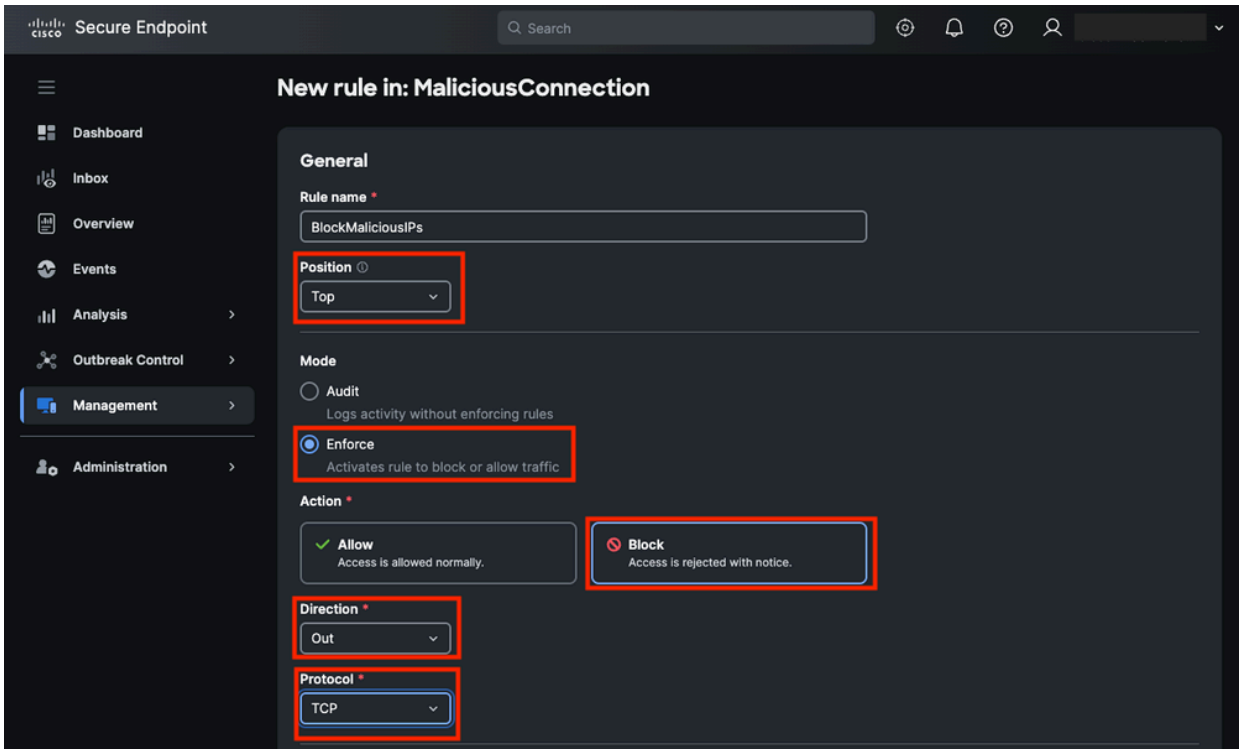
참고: 차단 규칙을 생성하지만 다른 트래픽이 합법적인 연결에 영향을 미치지 않도록 허용해야 합니다.

3. 기본 규칙이 생성되었는지 확인하고 Add Rule을 클릭합니다.

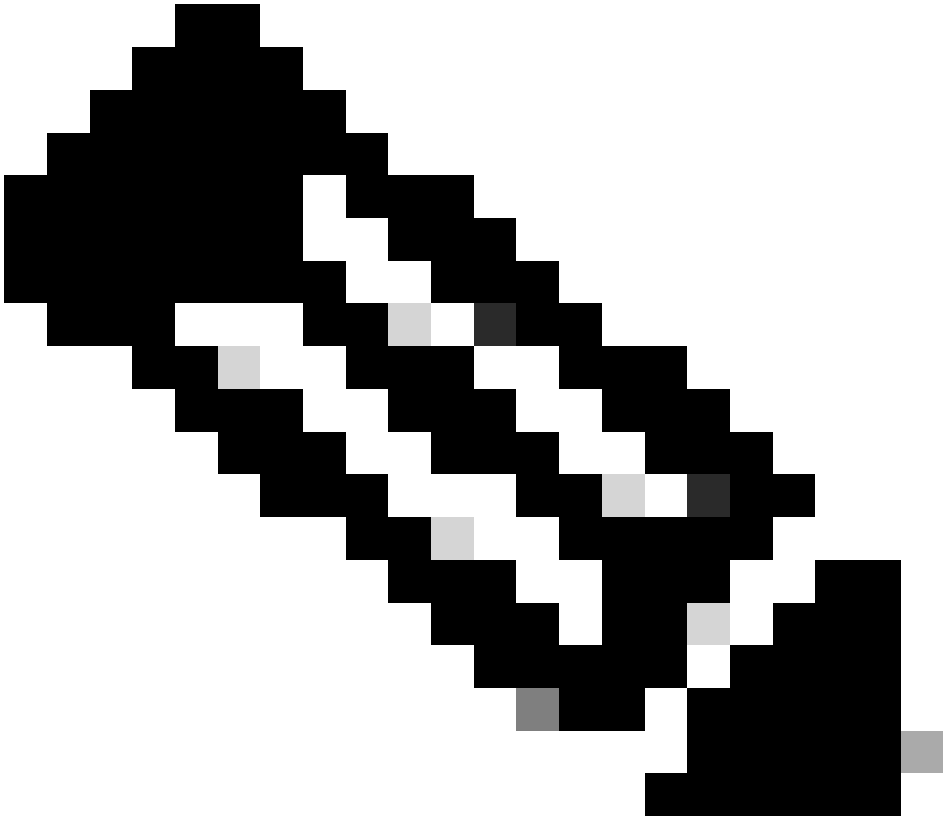


호스트 방화벽에 규칙 추가

4. 이름을 지정하고 다음 매개변수를 설정합니다.
   - 직무: 상단
   - 모드로 들어갑니다: 시행
   - 작업: 차단
   - 방향: 발신
   - 프로토콜: TCP


Secure Endpoint
Search
Dashboard
Inbox
Overview
Events
Analysis
Outbreak Control
Management
Administration
New rule in: MaliciousConnection
General
Rule name *
BlockMaliciousIPs
Position
Top
Mode
Audit
Logs activity without enforcing rules
Enforce
Activates rule to block or allow traffic
Action *
Allow
Access is allowed normally.
Block
Access is rejected with notice.
Direction *
Out
Protocol *
TCP

규칙 일반 매개변수



참고: 내부 엔드포인트에서 외부 대상, 일반적으로 인터넷으로의 악성 연결을 처리하는 경우 방향은 항상 Out일 수 있습니다.

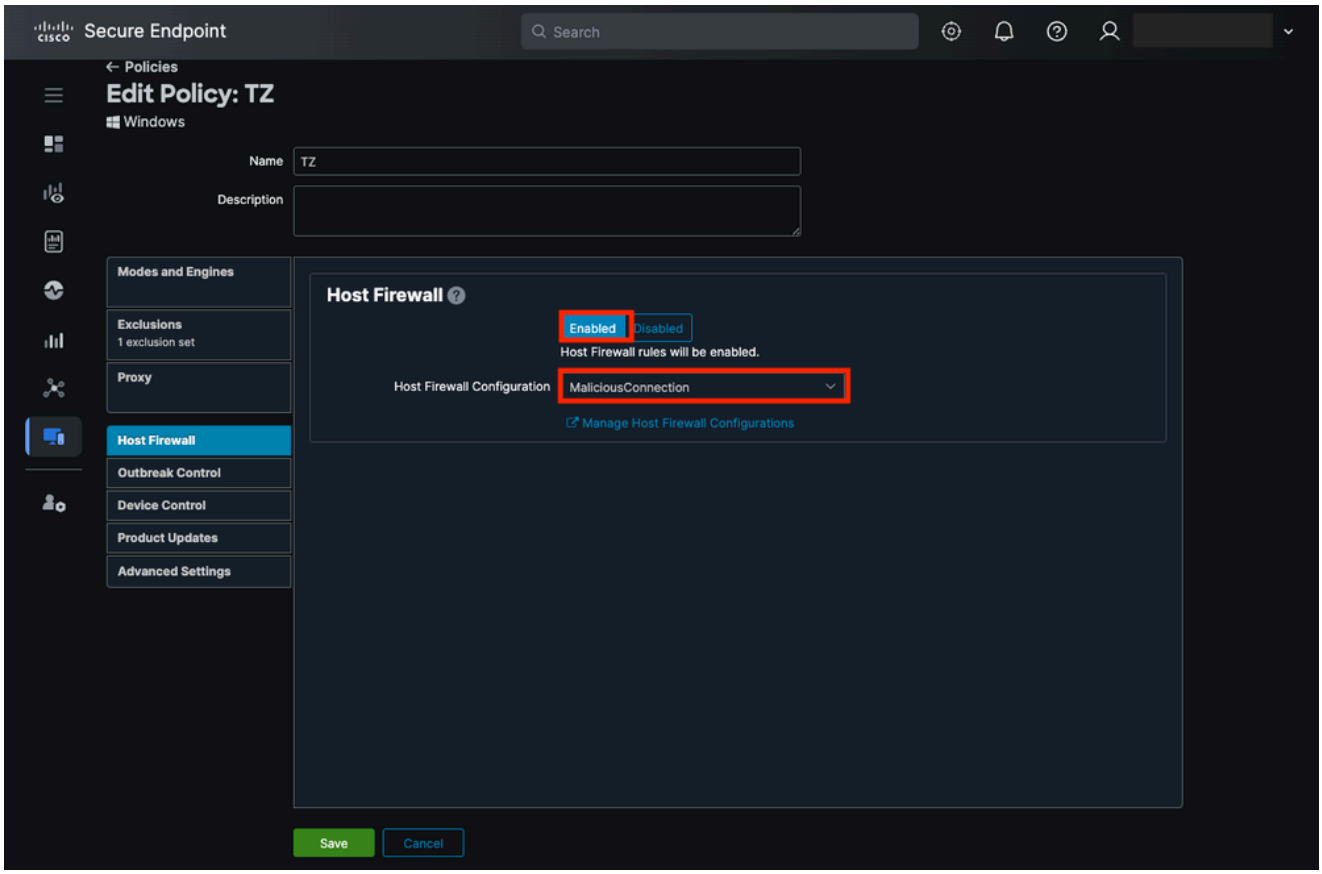
5. 로컬 및 대상 IP를 지정합니다.
   - 로컬 IP: 192.168.0.61
   - 원격 IP: 208.94.116.246
   - Local Portfield는 비워둡니다.
   - 대상 포트를 80 및 443으로 설정합니다. 이는 HTTP 및 HTTPS에 해당합니다.

규칙 주소 및 포트

6. 마지막으로 저장을 클릭합니다.

정책에서 호스트 방화벽 활성화 및 새 컨피그레이션 할당

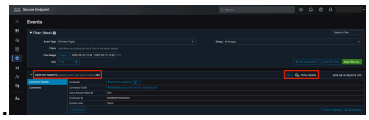
1. Secure Endpoint Portal(보안 엔드포인트 포털)에서 Management(관리) > Policies(정책)로 이동하고 악의적인 활동을 차단하려는 엔드포인트와 연결된 정책을 선택합니다.
2. 편집을 클릭하고 호스트 방화벽 탭으로 이동합니다.
3. 호스트 방화벽 기능을 활성화하고 최근 컨피그레이션(이 경우 MaliciousConnection)을 선택합니다.



보안 엔드포인트 정책에서 활성화된 호스트 방화벽

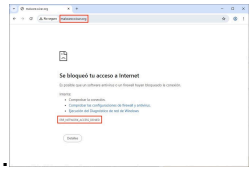
4. 저장을 클릭합니다.

5. 마지막으로 엔드포인트가 정책 변경 사항을 적용했는지 확인합니다.



정책 업데이트 이벤트

로컬에서 컨피그레이션 검증



1. 브라우저에서 URL malware.eicar.org를 사용하여 차단되었음을 확인합니다.

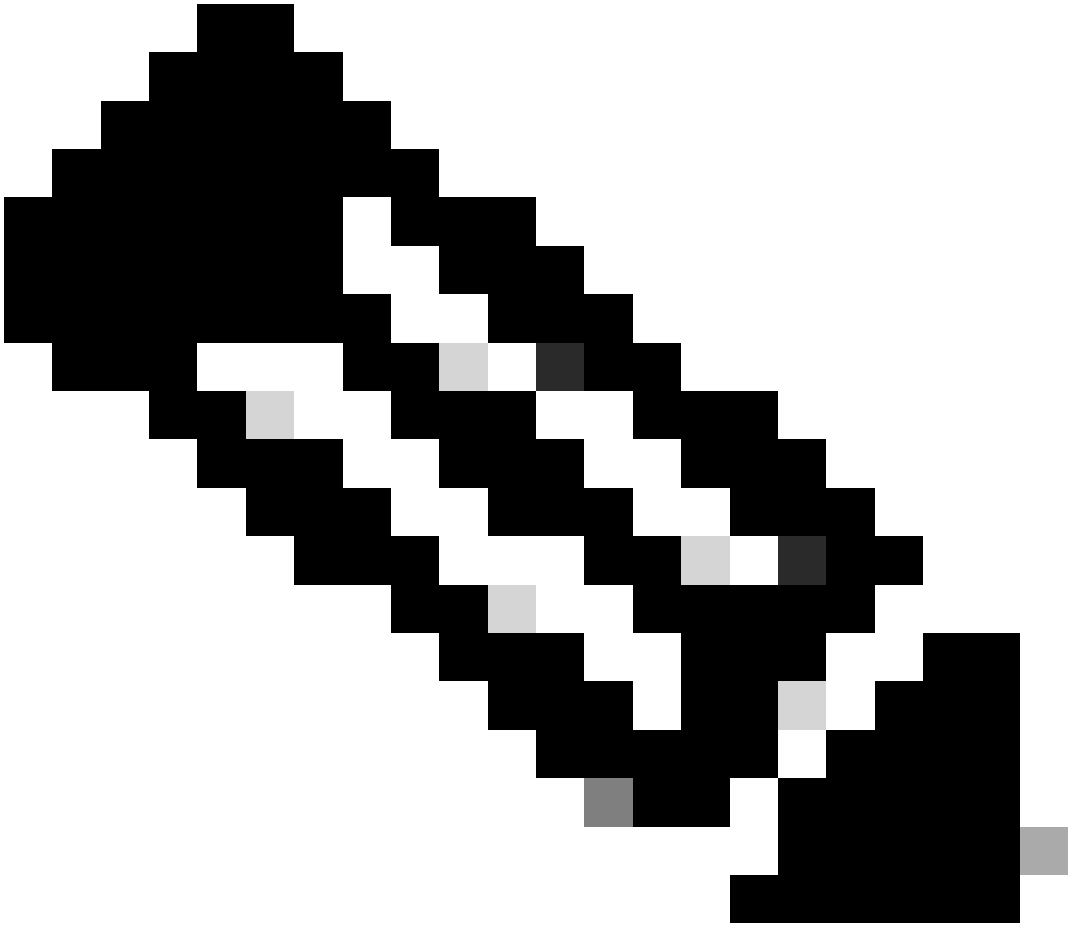
브라우저에서 네트워크 액세스가 거부되었습니다. 오류

2. 차단을 확인한 후 연결이 설정되지 않았는지 확인합니다. netstat -ano 명령을 사용합니다 | 악성 URL(208.94.116.246)과 연결된 IP가 표시되지 않도록 findstr이 설정되었습니다.

로그 검토

1. 엔드포인트에서 폴더로 이동합니다.

C:\Program Files\Cisco\AMP\<커넥터 버전>\FirewallLog.csv



참고: 로그 파일은 <install directory>\Cisco\AMP\<Connector version>\FirewallLog.csv 폴더에 있습니다.

---

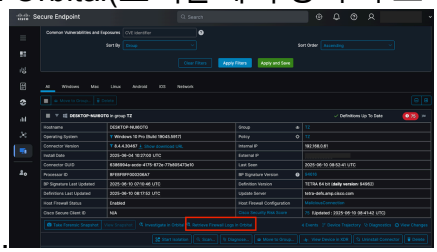
2. CSV 파일을 열어 차단 조치 규칙에 대한 일치를 검증합니다. 필터를 사용하여 허용 연결과 차단 연결을 구별합니다.

	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	

CSV 파일의 방화벽 로그

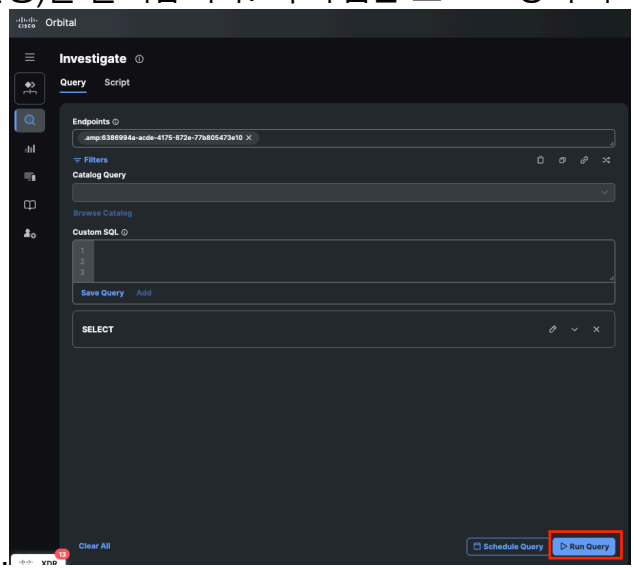
오비탈을 사용하여 방화벽 로그 검색

1. Secure Endpoint Portal(보안 엔드포인트 포털)에서 Management(관리) > Computers(컴퓨터)로 이동하고 엔드포인트를 찾은 다음 Retrieve Firewall Logs in Orbital(오비탈에서 방화벽 로그 검색)을 클릭합니다. 이 작업은 궤도 포털로 리디렉션됩니다.



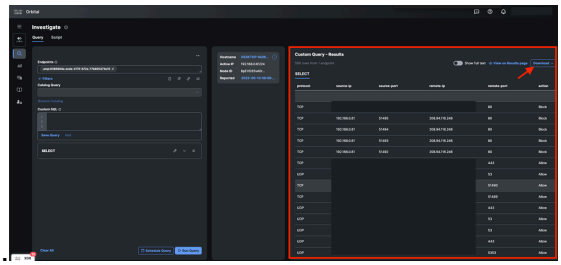
Orbital에서 방화벽 로그를 검색하는 버튼

2. Orbital Portal(궤도 포털)에서 Run Query(쿼리 실행)를 클릭합니다. 이 작업은 호스트 방화벽의 엔드포인트에 기록된 모든 로그를 표시합니다.



Orbital에서 쿼리 실행

3. 정보는 결과 탭에 표시되거나 다운로드할 수 있습니다.



Orbital의 쿼리 결과

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.