280-[SF] - 실습 - AWS Network Firewall을 사용한 맬웨어 예방

AWS Network Firewall을 사용한 맬웨어 예방

실습 개요

악성 소프트웨어를 의미하는 맬웨어는 사이버 범죄자(흔히 해커라고 함)가 데이터를 훔치고 컴퓨터와 컴퓨터 시스템에 해를 입히거나 손상시키기 위해 개발한 침입 소프트웨어를 지칭합니다. 일반적인 맬웨어에는 바이러스, 웜, 트로이 목마, 스파이웨어, 애드웨어, 랜섬웨어가 있습니다.

방화벽은 조직의 내부 네트워크와 인터넷 등 외부 퍼블릭 네트워크 사이에 보안을 위해 설치하는 물리적인 벽이라고 생각하면 됩니다. 방화벽은 외부 네트워크의 무단 사용자가 내부 네트워크에 액세스하지 못하도록 보호합니다.

사용자는 비즈니스를 위해 인터넷에 액세스가 필요하지만 무심코 맬웨어를 다운로드할 수 있고, 그렇게 되면 네트워크와 데이터 보안에 영향을 미칩니다.

현재 맬웨어 위협이 있을 수 있으며 조직에서는 다양한 기법과 서비스(예: 방화벽, 바이러스 백신 소프트웨어, 사용자 제어 모범 사례)를 사용하여 이러한 위협을 완화할 수 있습니다. 이 실습에서는 방화벽을 사용한 보호 조치에 중점을 둡니다.

시나리오

AnyCompany 는 새로운 보안 엔지니어로 여러분을 고용하고 회사의 보안 조치를 강화하는 임무를 맡겼습니다. 사용자들이 특정 웹 사이트에 액세스한 후 우연히 맬웨어를 다운로드했다는 보고가 있었습니다. AnyCompany 의 IT 팀에서는 여러분에게 맬웨어를 호스트하는 사이트의 URL 을 알려주었습니다. 여러분은 이런 악의적인 행위자의 파일에 액세스하지 못하도록 하는 솔루션을 찾아내야 합니다.

목표

이 실습을 마치면 다음을 수행할 수 있습니다.

- 네트워크 방화벽 업데이트
- 방화벽 규칙 그룹 생성
- 악성 사이트에 대한 액세스가 차단되었음을 확인 및 테스트

소요 시간

이 실습을 완료하려면 약 **45 분**이 소요됩니다.

실습 환경

이 실습에서는 사전에 구성된 **TestInstance**(Amazon Elastic Compute Cloud [Amazon EC2]) 인스턴스를 사용하여 악성 파일을 호스트하는 웹 사이트에 대한 액세스를 테스트합니다. 이 인스턴스는 경계 구역에 있으며 AnyCompany 의 나머지 중요한 서버와는 떨어져 있습니다. 여러분은 AnyCompany 네트워크 방화벽을 업데이트하고, 규칙 그룹을 생성한 후, 이 규칙 그룹을 방화벽 정책과 네트워크 방화벽에 연결합니다. 그런 다음 TestInstance 에 로그인하여 조치를 테스트합니다.

Amazon EC2, AWS Identity and Access Management(IAM) 역할, 일부 AWS 서비스 등 모든 백엔드 구성 요소는 이미 실습에 빌드되어 있습니다.

AWS 관리 콘솔 액세스

1. 이 지침의 오른쪽 상단에서 **Start Lab**(실습 시작)을 선택합니다.

   문제 해결 팁: **Access Denied**(액세스 거부됨) 오류가 나타날 경우 오류 메시지를 닫고 **Start Lab**(실습 시작)을 다시 선택합니다.

2. 다음 정보는 실습 상태를 나타냅니다.
   - 이 페이지 왼쪽 상단의 **AWS** 옆에 있는 빨간색 원은 실습이 시작되지 않았다는 것을 나타냅니다.
   - 이 페이지 왼쪽 상단의 **AWS** 옆에 있는 노란색 원은 실습이 시작된다는 의미입니다.
   - 이 페이지 왼쪽 상단의 **AWS** 옆에 있는 초록색 원은 실습이 준비되었다는 의미입니다.

   진행하기 전에 실습이 준비될 때까지 기다립니다.

3. 이 지침 상단에서 **AWS** 옆에 있는 초록색 원을 선택합니다.

   그러면 새 브라우저 탭에서 AWS 관리 콘솔이 열립니다. 시스템에 자동으로 로그인됩니다.

   팁: 새 브라우저 탭이 열리지 않는 경우 브라우저에서 팝업 창을 열 수 없음을 나타내는 배너 또는 아이콘이 브라우저 상단에 표시될 수도 있습니다. 배너 또는 아이콘을 선택하고 **Allow pop-ups**(팝업 허용)를 선택합니다.

4. 새로운 콘솔 홈으로 전환하라는 대화가 표시되면 **Switch to the new Console Home**(새 콘솔 홈으로 전환)을 선택합니다.
5. 이 지침과 함께 표시되도록 AWS 관리 콘솔 탭을 정렬합니다. 실습 단계를 수행할 수 있도록 두 브라우저 탭을 동시에 볼 수 있습니다.

   특별한 지시가 없는 한 실습 리전을 변경하지 마시기 바랍니다.

태스크 1: 연결성 확인

이 태스크에서는 실습 설정 시 구성된 EC2 인스턴스인 **TestInstance** 에 로그인합니다. 여기에서 IT 팀이 연결성 확인을 위해 여러분에게 제공한 악의적인 행위자 파일에 **wget** 명령을 실행합니다.

wget 은 무료 명령줄 유틸리티이자 네트워크 파일 다운로드 도구입니다.

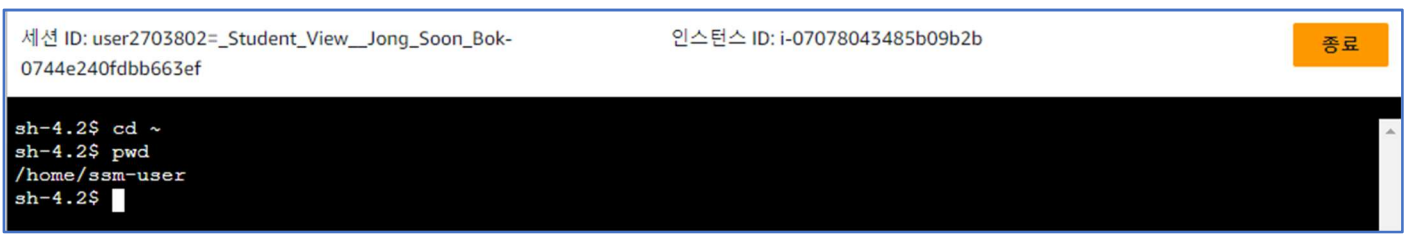
6. Vocareum 콘솔 페이지에서 **AWS Details**(AWS 세부 정보) 버튼을 선택합니다.
7. **TestInstanceURL** 옆에 링크가 있습니다. 이 링크를 복사하여 웹 브라우저의 새로운 탭에 붙여 넣습니다.

   이 링크로 이동하면 AWS Systems Manager 세션 관리자를 통해 TestInstance EC2 서버에 자동으로 로그인됩니다.

8. 디렉터를 변경하고 현재 사용 중인 디렉터리를 보려면 다음 명령을 실행합니다.

```
cd ~
pwd
```

다음 단계에서는 최종 사용자가 웹 브라우저를 사용하여 악성 파일을 다운로드하는 과정을 재현합니다. 이 작업은 명령줄에서 악성 파일에 **wget** 명령을 사용하여 시뮬레이션됩니다.



9. 보호된 이 실습 환경에서는 다음 코드를 입력하고 Enter 키를 눌러 맬웨어의 일부를 다운로드합니다.

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2023-09-13 04:55:15--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: 'js_crypto_miner.html'

100%[======================================================================>] 366         --.-K/s   in 0s

2023-09-13 04:55:15 (23.8 MB/s) - 'js_crypto_miner.html' saved [366/366]

sh-4.2$
```

10. 보호된 이 실습 환경에서는 다음 코드를 입력하고 Enter 키를 눌러 맬웨어의 나머지를 다운로드합니다.

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2023-09-13 04:55:53--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: 'java_jre17_exec.html'

100%[======================================================================>] 129         --.-K/s   in 0s

2023-09-13 04:55:53 (19.0 MB/s) - 'java_jre17_exec.html' saved [129/129]

sh-4.2$
```

팁: 각 코드 줄을 복사하여 붙여 넣은 후 Enter 키를 눌러야 모든 코드 줄을 실행할 수 있습니다.

이 파일은 맬웨어 방지 테스트와 학습을 위해 특별히 만들어진 것입니다. 보호된 이 실습 환경 외부에서 이 파일을 사용하지 마시기 바랍니다.

11. 다음과 비슷한 출력이 표시됩니다.

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2022-02-09 19:53:51--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: 'js_crypto_miner.html'

100%[=========================================================================================

2022-02-09 19:53:51 (49.3 MB/s) - 'js_crypto_miner.html' saved [366/366]

sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2022-02-09 19:53:53--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: 'java_jre17_exec.html'

100%[=========================================================================================

2022-02-09 19:53:53 (17.4 MB/s) - 'java_jre17_exec.html' saved [129/129]
```

12. 다운로드한 파일을 보려면 다음 명령을 실행합니다.

```
ls
```

출력은 다음 이미지와 같이 표시됩니다.

```
sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$
```

태스크 1 요약

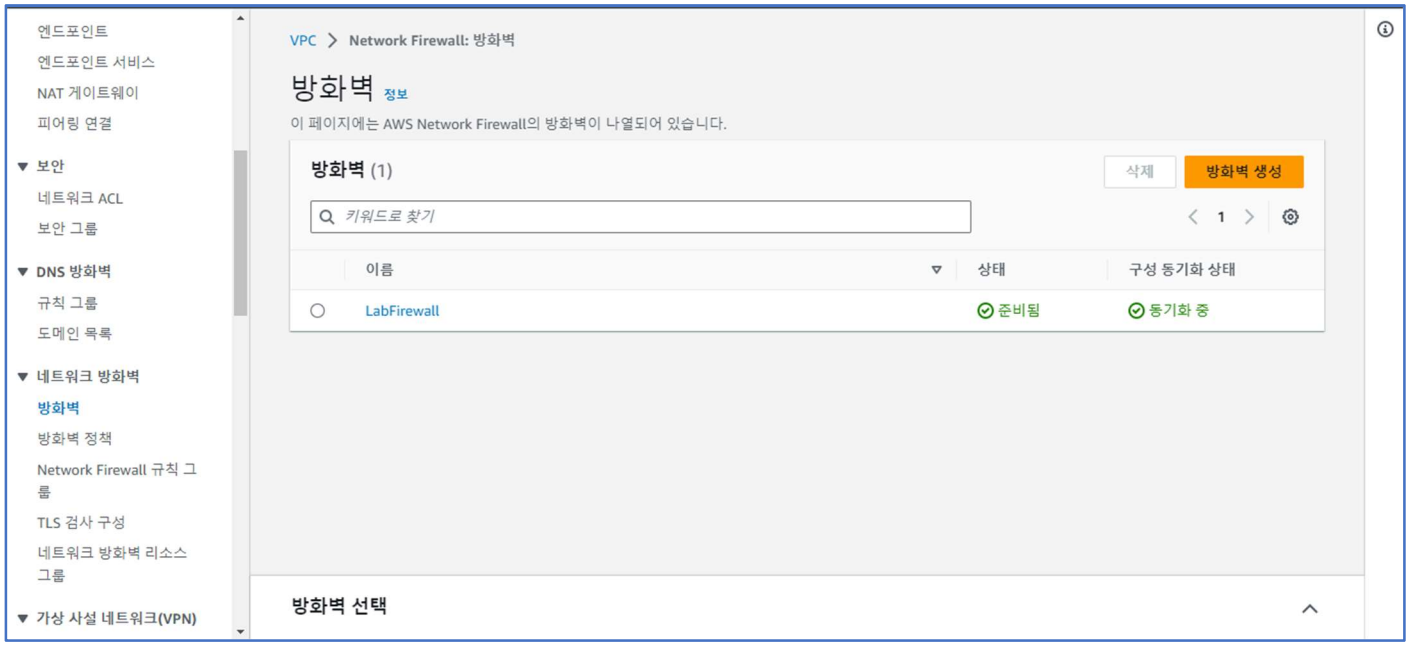
이 태스크에서는 AnyCompany 에서 사용하는 현재 네트워크와 네트워크 방화벽을 통해 악성 파일을 호스트하는 URL 에 액세스할 수 있음을 확인했습니다. 격리된 TestInstance EC2 인스턴스를 사용하여 명령을 실행하고 사용자가 다운로드한 것과 같은 악성 파일을 다운로드했습니다. 이제 AnyCompany 네트워크 방화벽을 수정하여 이 사이트에 대한 액세스를 막아야 합니다.

태스크 2: 네트워크 방화벽 점검

이 태스크에서는 실습 설정 시 구성된 AWS Network Firewall **방화벽**을 점검합니다. 신규 보안 엔지니어인 여러분에게 AnyCompany 가 맡긴 임무 중에서 이 방화벽을 업데이트하는 것이 가장 중요합니다.

13. AWS 관리 콘솔에서 검색 창에 **VPC** 를 입력한 후 **VPC** 를 선택합니다.

14. 왼쪽 탐색 창의 **NETWORK FIREWALL**(네트워크 방화벽)에서 **Firewalls**(방화벽)를 선택합니다.



~~15. **LabFirewall** 을 선택한 후 **Overview**(개요) 섹션에 있는 세 단계를 모두 읽습니다.~~

16. **Step 2: Configure the firewall policy**(2 단계: 방화벽 정책 구성)에서 **LabFirewallPolicy** 링크를 선택하여 관련 정책을 엽니다.

방화벽 정책은 스테이트리스 및 스테이트풀 규칙 그룹과 기타 설정의 모음을 통해 방화벽의 동작을 정의합니다.

17. **Stateless default actions**(스테이트리스 기본 작업) 섹션에서 **Edit**(편집)을 선택합니다.

18. **Stateless default actions**(스테이트리스 기본 작업)에서 다음 옵션을 구성합니다.
    - **Choose how to treat fragmented packets**(분열된 패킷을 처리하는 방법 선택): **Use the same actions for all packets**(모든 패킷에 같은 작업 사용)를 선택합니다.
    - **Action**(작업): **Forward to stateful rule groups**(스테이트풀 규칙 그룹으로 전달)를 선택합니다.

19. **Save**(저장)를 선택합니다.

    이 설정은 이제 향후 점검을 위해 모든 패킷을 스테이트풀 규칙 그룹으로 전달합니다.

스테이트풀 규칙 엔진은 트래픽 흐름의 맥락에서 패킷을 점검하고, 더 복잡한 규칙을 사용할 수 있게 해주며, 네트워크 트래픽과 트래픽에 대한 AWS Network Firewall 방화벽 경고를 로깅할 수 있게 해줍니다. 스테이트풀 규칙은 트래픽 방향을 고려합니다. 스테이트풀 규칙 엔진은 점검을 위해 그룹 패킷으로의 패킷 전달을 지연시킬 수 있습니다.

스테이트리스 규칙 엔진은 트래픽 방향이나 패킷이 기존의 승인된 연결의 일부인지 등의 요인과 상관없이 각 패킷을 개별적으로 점검합니다. 이 엔진은 평가의 속도를 우선시합니다.

태스크 2 요약

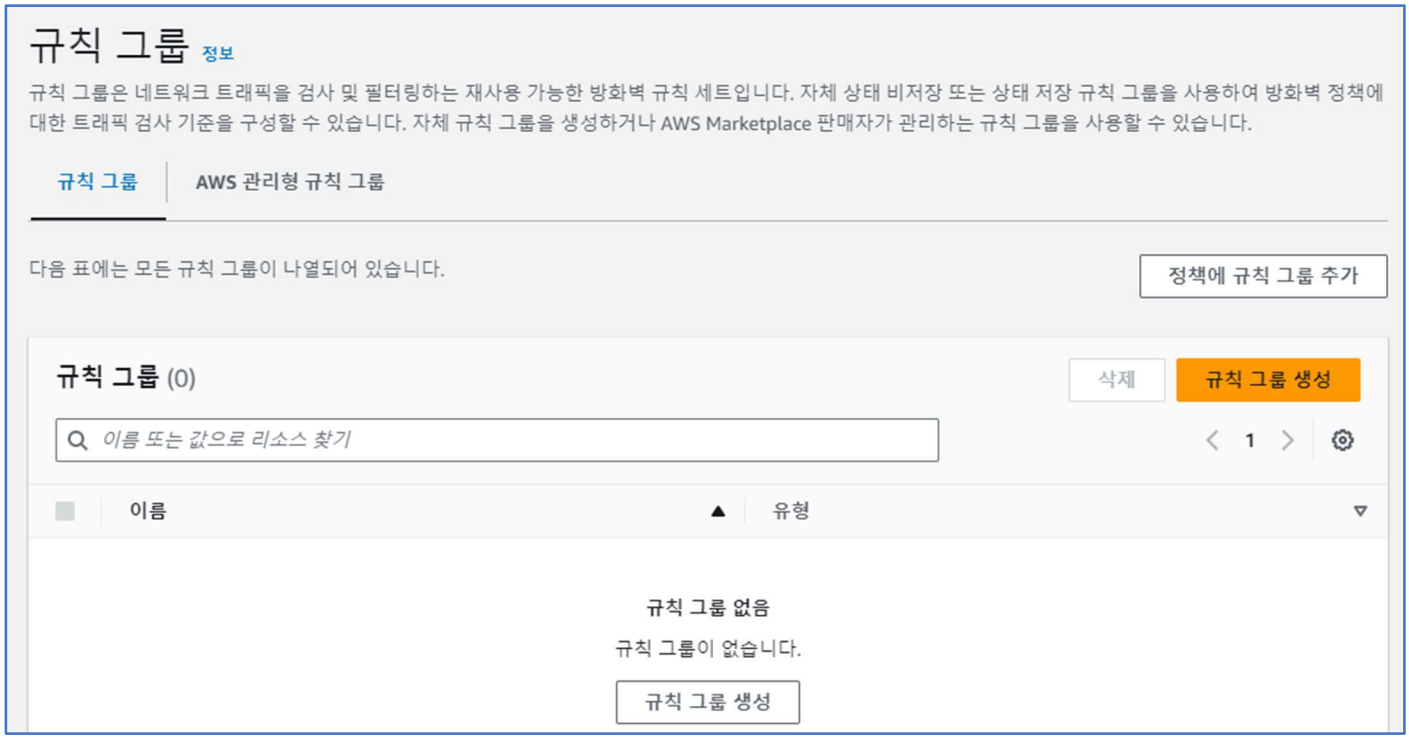
이 태스크에서는 네트워크 방화벽을 점검하고 방화벽 정책을 업데이트했습니다. 그런 다음, 스테이트풀 규칙 점검을 위해 모든 패킷을 전달하도록 방화벽 정책을 업데이트했습니다.

태스크 3: 방화벽 규칙 그룹 생성

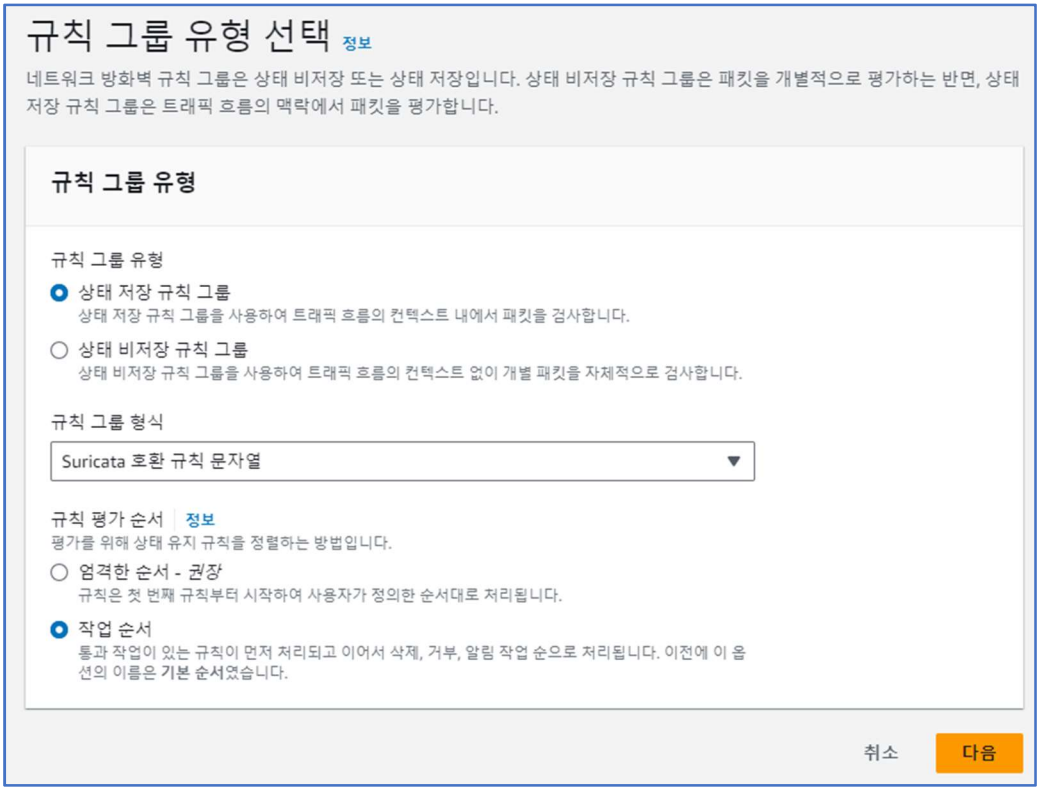
이 태스크에서는 악성 URL 에 대한 액세스를 차단하는 규칙으로 네트워크 방화벽 규칙 그룹을 생성합니다. 그런 다음, 이 규칙 그룹을 방화벽 정책에 연결합니다.

네트워크 방화벽 규칙 그룹은 네트워크 트래픽을 점검하고 처리하기 위해 재사용할 수 있는 기준의 세트입니다. 정책 구성 시 방화벽 정책에 하나 이상의 규칙 그룹을 추가합니다. 이 규칙 그룹은 악의적인 행위자 URL 에 대한 액세스를 차단합니다.

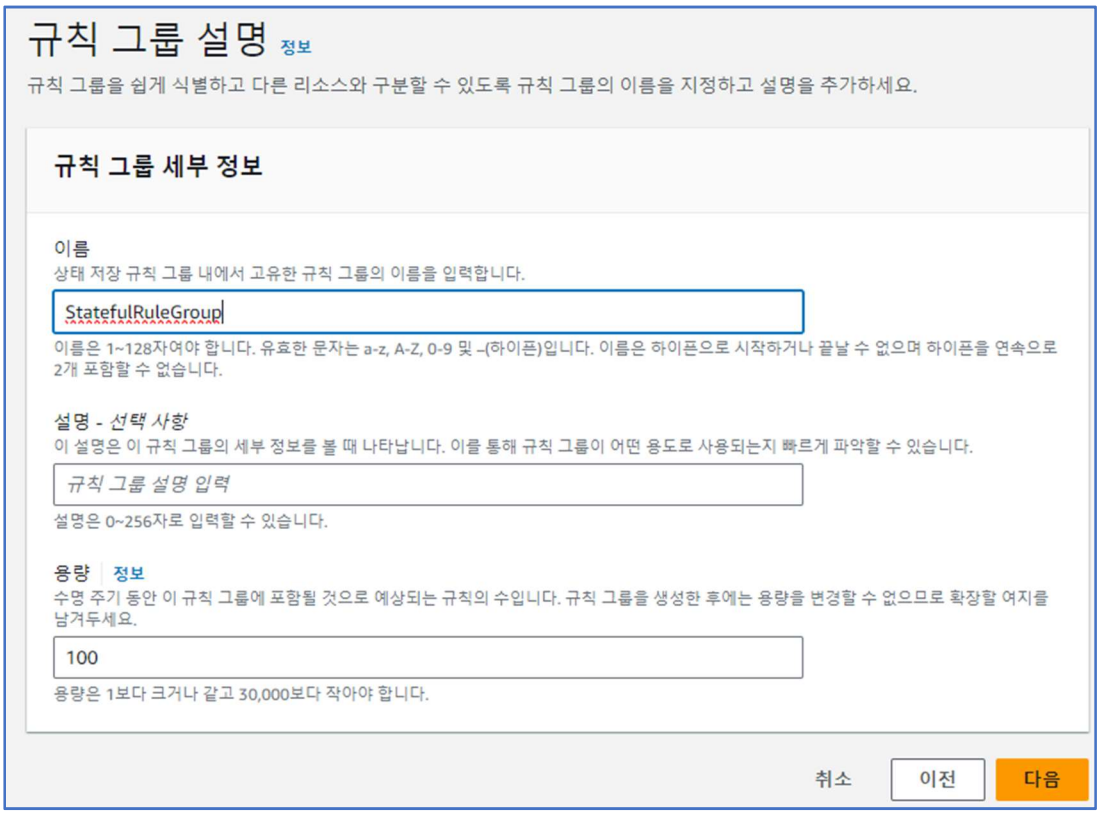
20. 왼쪽 탐색 창의 **NETWORK FIREWALL**(네트워크 방화벽)에서 **Network Firewall Rule Groups**(네트워크 방화벽 규칙 그룹)를 선택합니다.
21. **Create Network Firewall rule group**(네트워크 방화벽 규칙 그룹 생성)을 선택합니다.



22. **Create Network Firewall rule group**(네트워크 방화벽 규칙 그룹 생성) 섹션에서 다음 옵션을 구성합니다.
    - **Rule group type**(규칙 그룹 유형)에서 **Stateful rule group**(스테이트풀 규칙 그룹)을 선택합니다.



- **Stateful rule group**(스테이트풀 규칙 그룹) 섹션에서 다음 옵션을 구성합니다.
  - **Name**(이름): `StatefulRuleGroup` 을 입력합니다.
  - **Capacity**(용량): `100` 을 입력합니다.
  - **Stateful rule group options**(스테이트풀 규칙 그룹 옵션): **Suricata compatible IPS rules**(Suricata 호환 IPS 규칙)를 선택합니다.



침입 방지 시스템(IPS) 규칙은 Suricata 규칙 구문을 사용하여 더 강화된 방화벽 규칙을 제공합니다. Suricata 는 오픈 소스 네트워크 IPS 로, 트래픽 점검을 위한 표준 규칙 기반 언어를 포함합니다.

23. **Suricata compatible IPS rules**(Suricata 호환 IPS 규칙) 섹션에서 다음 코드를 텍스트 상자에 입력합니다.

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002001;
content:"/data/js_crypto_miner.html";http_uri; rev:1;)

drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002002;
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

트래픽이 **LabVPC** 에서 시작해서 퍼블릭 네트워크로 이동할 때 지금 추가한 두 개의 Suricata 규칙이 **http_uri contents /home/ssm-user/js_crypto_miner.html** and **http_uri contents /home/ssm-user/js_crypto_miner.html** URL 과 일치하는 트래픽을 차단합니다.

24. **Create stateful rule group**(스테이트풀 규칙 그룹 생성)을 선택합니다.

고급 설정 구성 - *선택 사항* 정보

고객 관리형 AWS Key Management Service(KMS) 키를 구성하여 리소스를 암호화 및 복호화합니다.

고객 관리형 키 - *선택 사항* 정보

AWS Key Management(KMS)에서 고객 관리형 키를 사용하여 저장 데이터를 암호화할 수 있습니다. 고객 관리형 키를 구성하지 않는 경우 Network Firewall은 AWS 관리형 키를 사용하여 데이터를 암호화합니다.

데이터는 기본적으로 AWS에서 소유하고 자동으로 관리하는 키로 암호화됩니다. 다른 키를 선택하려면 암호화 설정을 사용자 지정합니다.

☐ 암호화 설정 사용자 지정(고급)

취소 | 이전 | 다음

검토 및 생성 정보

1단계: 규칙 그룹 유형

편집 1단계

규칙 그룹 유형

규칙 그룹 유형	상태 저장 규칙 그룹 옵션	규칙 순서
상태 저장	Suricata compatible rule string	default

2단계: 규칙 그룹

편집 2단계

규칙 그룹 세부 정보

이름	설명	용량
StatefulRuleGroup	-	100

생성 완료 규칙 그룹 StatefulRuleGroup.

VPC > 네트워크 방화벽: 규칙 그룹

규칙 그룹 정보

규칙 그룹은 네트워크 트래픽을 검사 및 필터링하는 재사용 가능한 방화벽 규칙 세트입니다. 자체 상태 비저장 또는 상태 저장 규칙 그룹을 사용하여 방화벽 정책에 대한 트래픽 검사 기준을 구성할 수 있습니다. 자체 규칙 그룹을 생성하거나 AWS Marketplace 판매자가 관리하는 규칙 그룹을 사용할 수 있습니다.

규칙 그룹 | AWS 관리형 규칙 그룹

다음 표에는 모든 규칙 그룹이 나열되어 있습니다.

정책에 규칙 그룹 추가

규칙 그룹 (1)

삭제 | 규칙 그룹 생성

이름 또는 값으로 리소스 찾기

1

☐	이름 ▲	유형 ▽
☐	StatefulRuleGroup	Stateful

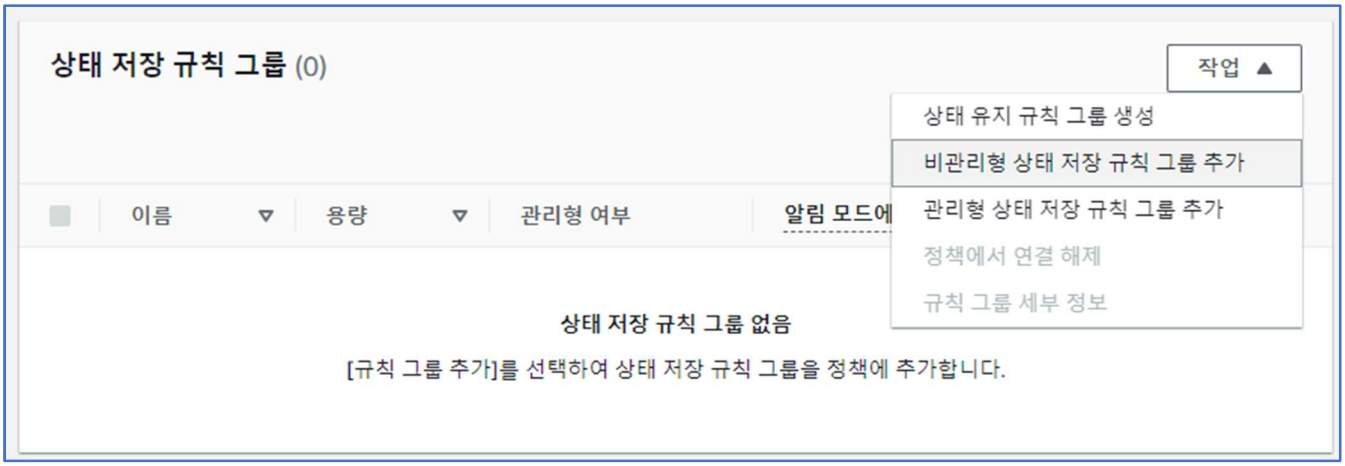
태스크 3 요약

이 태스크에서는 Suricata 규칙을 사용하는 스테이트풀 네트워크 방화벽 규칙 그룹을 생성했습니다. 이 규칙 그룹을 네트워크 방화벽에 연결하면 AnyCompany 사용자가 액세스했던 악성 웹 사이트가 차단됩니다.

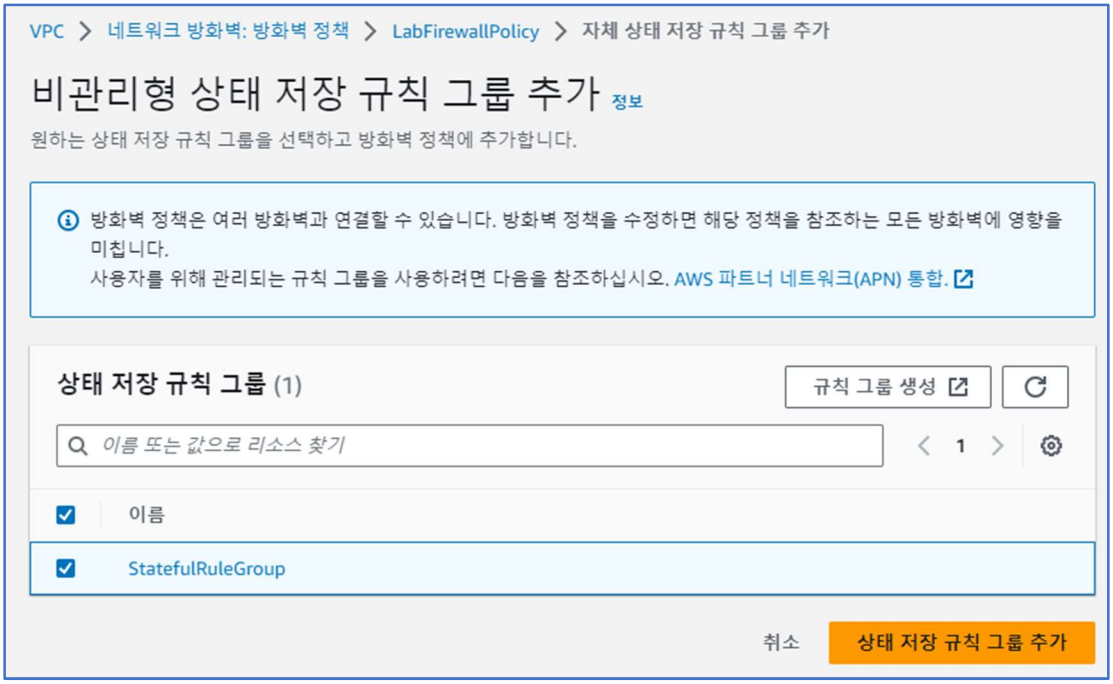
태스크 4: 네트워크 방화벽에 규칙 그룹 연결

이 태스크에서는 조금 전에 생성한 네트워크 방화벽 규칙 그룹을 네트워크 방화벽에 연결합니다.

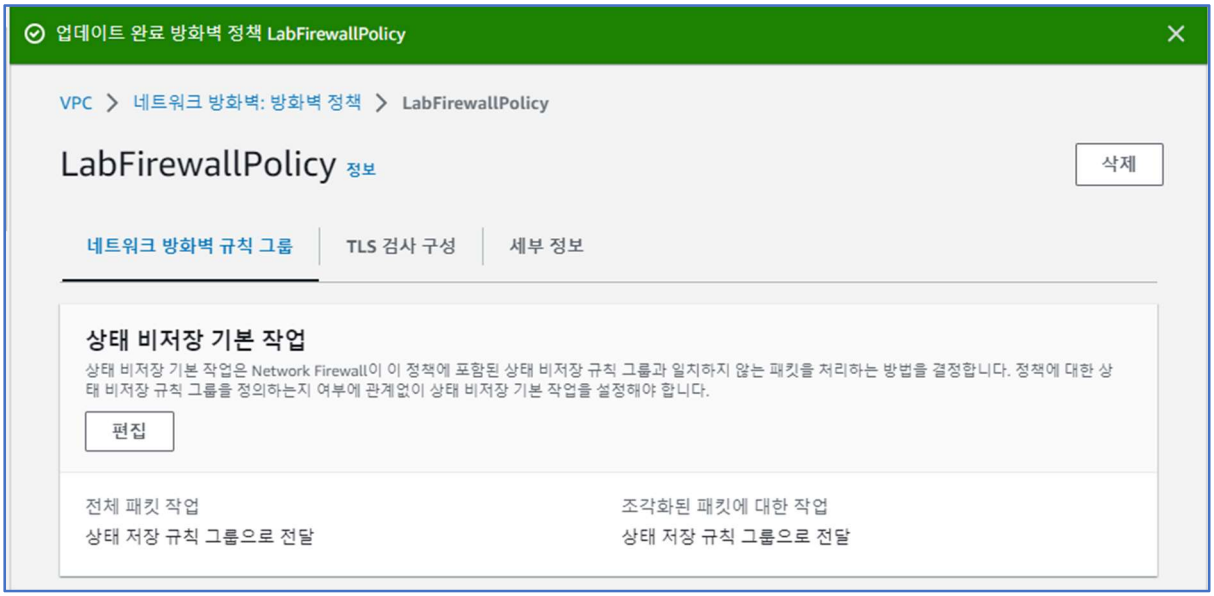
25. 왼쪽 탐색 창의 **NETWORK FIREWALL**(네트워크 방화벽)에서 **Firewalls**(방화벽)를 선택합니다.
26. **LabFirewall** 을 선택합니다.
27. **Step 2**(2 단계)에서 **Add rule groups**(규칙 그룹 추가) 드롭다운 목록을 선택하고 **Add from existing stateful rule groups**(기존 스테이트풀 규칙 그룹에서 추가)를 선택합니다.



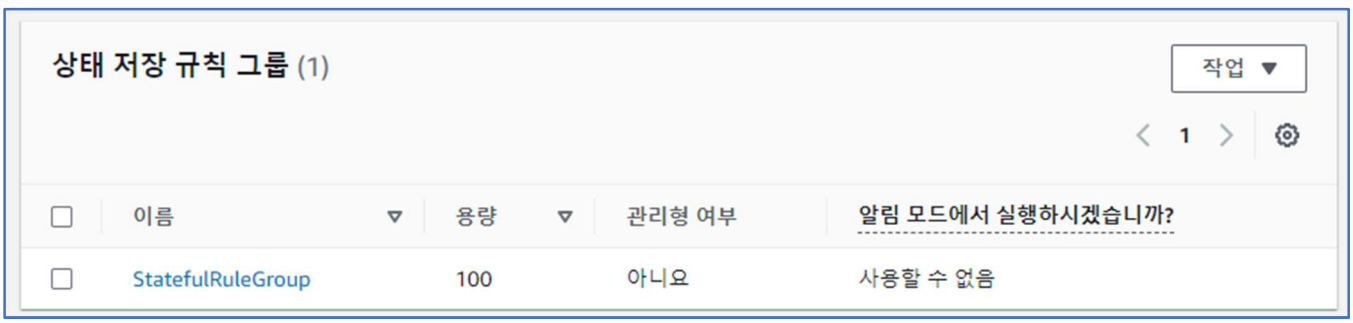
28. **StatefulRuleGroup** 의 확인란을 선택한 후 **Add stateful rule group**(스테이트풀 규칙 그룹)을 선택합니다.



페이지 상단에 **You successfully updated FirewallPolicy**(FirewallPolicy 를 업데이트했습니다)라는 초록색 배너가 표시될 것입니다.



29. **Stateful rule groups**(스테이트풀 규칙 그룹) 섹션으로 스크롤하여 추가된 방화벽 규칙 그룹을 확인합니다.



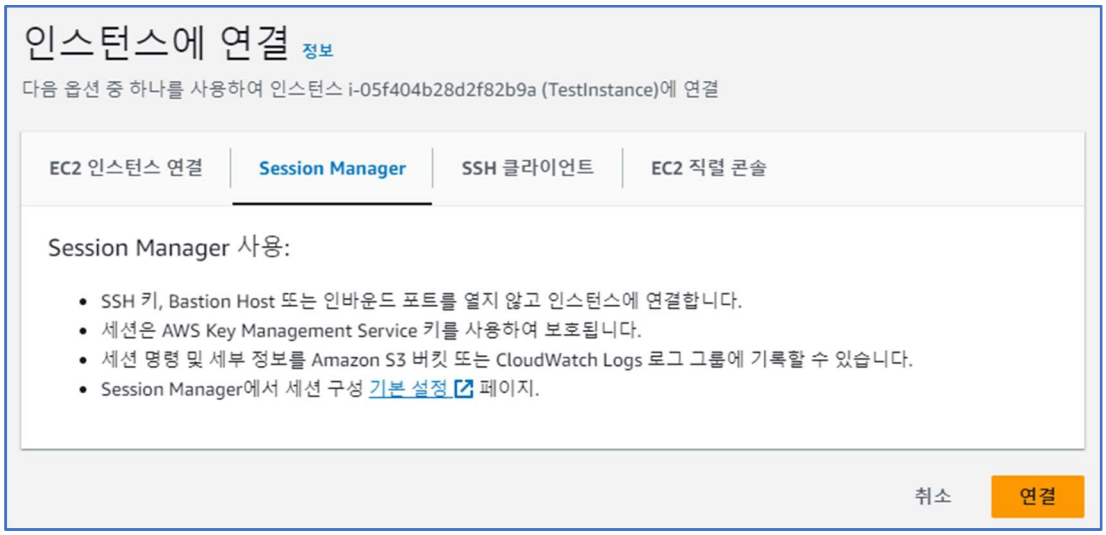
태스크 4 요약

규칙 그룹을 방화벽에 연결했습니다. 이 방화벽이 웹 사이트에서 호스트되는 악의적인 행위자 파일에 대한 액세스 시도를 차단합니다.

태스크 5: 솔루션 검증

이 태스크에서는 다시 TestInstance 에 로그인하여 네트워크 방화벽이 악성 웹 사이트 파일에 대한 액세스 시도를 제대로 차단하는지 테스트합니다.

30. AWS 관리 콘솔에서 검색 창에 **EC2** 를 입력한 후 **EC2** 를 선택합니다.
31. 왼쪽 탐색 창에서 **Instances**(인스턴스)를 선택합니다.
32. **TestInstance** 옆의 확인란을 선택한 후 **Connect**(연결)를 선택합니다.
33. **Session Manager**(세션 관리자) 탭을 선택하고 **Connect**(연결)를 선택합니다.



34. 디렉터를 변경하고 현재 사용 중인 디렉터리를 보려면 다음 명령을 실행합니다.

```
cd ~
pwd
```

35. 첫 번째 악성 파일에 액세스를 시도하려면 다음 **wget** 명령을 실행합니다.

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

출력이 다음과 같이 표시됩니다.

```
HTTP request sent, awaiting response...
```

이 출력은 맬웨어 사이트와 파일에 더 이상 액세스할 수 없으며 네트워크 방화벽이 성공적으로 차단한다는 것을 보여줍니다.

36. Ctrl+c 를 눌러 명령을 중지합니다.
37. 다른 악성 URL 에 대한 액세스를 테스트하려면 다음 명령을 실행합니다.

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

출력이 다음과 같이 표시됩니다.

```
HTTP request sent, awaiting response...
```

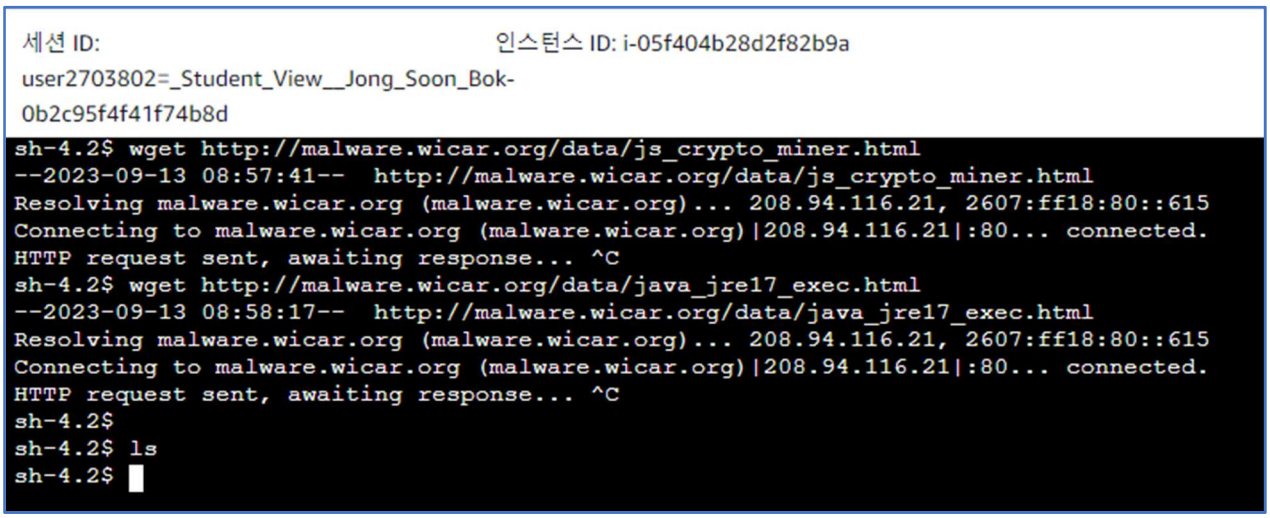
38. 다음으로, 테스트 맬웨어 파일을 제거하려면 다음 명령을 실행합니다.

```
rm java_jre17_exec.html js_crypto_miner.html
```

39. 파일이 삭제되었는지 확인하려면 **ls** 명령을 실행합니다.

```
ls
```

출력이 비어 있을 것입니다. 파일이 제거되었다는 뜻입니다.



태스크 5 요약

이 태스크에서는 네트워크 방화벽이 업데이트되었으며 악성 웹 사이트를 차단하도록 올바르게 구성되었는지 확인했습니다. TestInstance EC2 인스턴스에 로그인하고 이 파일에 **wget** 명령을 실행하여 액세스가 차단되는 것을 확인했습니다. 이제 사용자가 이 웹 사이트에서 이러한 악성 파일에 액세스할 수 없습니다.

마무리

축하합니다! 지금까지 다음 태스크를 완료했습니다.

- 네트워크 방화벽 업데이트
- 방화벽 규칙 그룹 생성
- 악성 사이트에 대한 액세스가 차단되었음을 확인 및 테스트

실습 완료

40. 이 페이지의 상단에서 **End Lab**(실습 종료)을 선택하고 **Yes**(예)를 선택하여 실습 종료를 확인합니다.
41. **Ended AWS Lab Successfully**(AWS Lab 이 종료되었습니다)라는 메시지가 잠시 표시되어 실습이 종료되었음을 나타냅니다.

AWS Training and Certification 에 대한 자세한 내용은 AWS Training and Certification 을 참조하십시오.

여러분의 피드백을 환영합니다.

제안이나 수정 사항을 공유하려면 AWS Training and Certification 문의 양식에 세부 정보를 제공해 주십시오.

Malware Protection Using an AWS Network Firewall

Lab overview

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan horses, spyware, adware, and ransomware.

Firewalls are like physical security walls situated between an organization's internal network and any external public networks such as the internet. The firewall protects an internal network from access by unauthorized users on an external network.

Users need access to the internet for business reasons, but they can inadvertently download malware, which can impact network and data security.

Malware threats can be present, and organizations can use various techniques and services to mitigate these threats (for example, firewalls, antivirus software, and user control best practice). This lab focuses on countermeasure techniques using a firewall.

Scenario

AnyCompany has hired you as a new security engineer, and the company has tasked you with hardening the company's security perimeter. There have been reports of users accidentally downloading malware after accessing specific websites. The IT team for AnyCompany has provided you with the URLs of the sites hosting the malware. It is your job to find a solution to mitigate access to these malicious actor files.

Objectives

After completing this lab, you should be able to:

- Update a network firewall
- Create a firewall rules group
- Verify and test that access to malicious sites is blocked

Duration

This lab requires approximately **45 minutes** to complete.

Lab environment

In this lab, you have a pre-configured **TestInstance** (Amazon Elastic Compute Cloud [Amazon EC2]) instance to use to test access to the website hosting malicious files. This is contained in a perimeter zone and separated from the rest of AnyCompany's important servers. You update the AnyCompany network firewall, create a rules group, and then attach that rules group to a firewall policy and the network firewall itself. You then log into the TestInstance and test the remediation.

All backend components, such as Amazon EC2, AWS Identity and Access Management (IAM) roles, and some AWS services, have been built into the lab already.

Accessing the AWS Management Console

1. At the upper-right corner of these instructions, choose **Start Lab**

   Troubleshooting tip: If you get an **Access Denied** error, close the error box, and choose **Start Lab** again.

2. The following information indicates the lab status:
   - A red circle next to **AWS** at the upper-left corner of this page indicates that the lab has not been started.
   - A yellow circle next to **AWS** at the upper-left corner of this page indicates that the lab is starting.
   - A green circle next to **AWS** at the upper-left corner of this page indicates that the lab is ready.

   Wait for the lab to be ready before proceeding.

3. At the top of these instructions, choose the green circle next to **AWS**

   This option opens the AWS Management Console in a new browser tab. The system automatically sign you in.

   Tip: If a new browser tab does not open, a banner or icon at the top of your browser might indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

4. If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.
5. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you should be able to see both browser tabs at the same time so that you can follow the lab steps.

   Do not change the lab Region unless specifically instructed to do so.

Task 1: Confirm Reachability

In this task, you log into the EC2 instance **TestInstance** that has been pre-configured during lab setup. From there, you issue a **wget** command to the malicious actor files that the IT team provided to you to confirm reachability.

wget is a free command-line utility and network file downloader.

6. From the Vocareum console page, choose the **AWS Details** button.
7. Next to **TestInstanceURL**, there is a link. Copy and paste the link into a new tab in your web browser.

   This link directly logs you into the TestInstance EC2 server via AWS Systems Manager Session Manager.

8. To change directories and view the current working directory, run the following commands:

```
cd ~
pwd
```

The next step replicates how an end user would download a malicious file using a web browser. This action is simulated using the **wget** command on the malicious files in the command line.

9. In this protected lab environment, enter the following code and press Enter to download part of the malware:

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

10. In this protected lab environment, enter the following code and press Enter to download the rest of the malware:

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

Tip: Make sure to press Enter after copying and pasting each line of code to ensure that you run both lines of code.

These files are made specifically for anti-malware testing purposes and learning. Do not use them outside of this protected lab environment.

11. You should see an output similar to the following:

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2022-02-09 19:53:51--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: 'js_crypto_miner.html'

100%[=======================================================================================

2022-02-09 19:53:51 (49.3 MB/s) - 'js_crypto_miner.html' saved [366/366]

sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2022-02-09 19:53:53--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: 'java_jre17_exec.html'

100%[=======================================================================================

2022-02-09 19:53:53 (17.4 MB/s) - 'java_jre17_exec.html' saved [129/129]
```

12. To view the downloaded files, run the following command:

```
ls
```

The output should look like the following image:

```
sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$
```

Summary of task 1

In this task, you confirmed that the URL hosting the malware files is accessible through the current network and network firewall that AnyCompany is using. You used an isolated TestInstance EC2 instance to run commands and download the same malicious files that users downloaded. You now need to fix the AnyCompany network firewall to stop access to this site.

Task 2: Inspect the network firewall

In this task, you inspect the AWS Network Firewall **firewall** that was pre-configured during lab setup. Updating this firewall is the top priority that AnyCompany has issued to you as the new security engineer.

13. In the AWS Management Console, enter **VPC** in the search bar, and then choose **VPC**.
14. In the left navigation pane under **NETWORK FIREWALL**, choose **Firewalls**.
15. Choose **LabFirewall**, and read through the three steps in the **Overview** section.
16. In **Step 2: Configure the firewall policy**, choose the **LabFirewallPolicy** link to open the associated policy.

    A firewall policy defines the behavior of the firewall in a collection of stateless and stateful rule groups and other settings.

17. In the **Stateless default actions** section, choose **Edit**.
18. For **Stateless default actions**, configure the following options:
    - **Choose how to treat fragmented packets**: Choose **Use the same actions for all packets**.
    - **Action**: Choose **Forward to stateful rule groups**.
19. Choose **Save**.

    These settings now forward all packets to a stateful rule group for further inspection.

    A stateful rules engine inspects packets in the context of their traffic flow, gives you the ability to use more complex rules, and gives you the ability to log network traffic and AWS Network Firewall firewall alerts on traffic. Stateful rules consider traffic direction. The stateful rules engine might delay packet delivery to group packets for inspection.

    A stateless rules engine inspects each packet in isolation without regard to factors such as the direction of traffic or whether the packet is part of an existing, approved connection. This engine prioritizes the speed of evaluation.

Summary of task 2

In this task, you inspected the network firewall and updated the firewall policy. You then updated the firewall policy to forward all packets for stateful rule inspection.

Task 3: Create a firewall rule group

In this task, you create a network firewall rule group with rules that block access to the malicious URLs. You later attach this rule group to your firewall policy.

A network firewall rule group is a reusable set of criteria for inspecting and handling network traffic. You add one or more rule groups to a firewall policy as part of policy configuration. This rule group blocks access to the malicious actor URLs.

20. In the left navigation pane under **NETWORK FIREWALL**, choose **Network Firewall Rule Groups**.
21. Choose **Create Network Firewall rule group**.
22. In the **Create Network Firewall rule group** section, configure the following options:
    - For **Rule group type**, choose **Stateful rule group**.
    - In the **Stateful rule group** section, configure the following options:
        - **Name**: Enter `StatefulRuleGroup`
        - **Capacity**: Enter `100`
        - **Statefule rule group options**: Choose **Suricata compatible IPS rules**.

    Intrusion prevention system (IPS) rules provide advanced firewall rules using Suricata rule syntax. Suricata is an open-source network IPS that includes a standard rule-based language for traffic inspection.

23. In the **Suricata compatible IPS rules** section, enter the following code into the text box:

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002001;
content:"/data/js_crypto_miner.html";http_uri; rev:1;)

drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002002;
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

    The two Suricata rules that you added now block traffic that matches the **http_uri contents /data/js_crypto_miner.html** and **http_uri contents /data/js_crypto_miner.html** URLs when the traffic is initiated from the **LabVPC** to the public network.

24. Choose **Create stateful rule group**.

Summary of task 3

In this task, you created a stateful network firewall rule group that uses Suricata rules. Once you attach this rule group to the network firewall, it blocks the malicious websites that AnyCompany users accessed.

Task 4: Attach a rule group to the network firewall

In this task, you attach the network firewall rule group that you created to the network firewall.

25. In the left navigation pane under **NETWORK FIREWALL**, choose **Firewalls**.
26. Choose **LabFirewall**.
27. Under **Step 2**, select the **Add rule groups** dropdown list, and then choose **Add from existing stateful rule groups**.
28. Select the check box for **StatefulRuleGroup**, and then choose **Add stateful rule group**.

    At the top of the page, you should see a green **You successfully updated FirewallPolicy** banner.

29. Scroll to the **Stateful rule groups** section to see the successfully added firewall rule group.

Summary of task 4

You have attached the rule group to the firewall, which blocks attempts to access the malicious actor files hosted within the website.

Task 5: Validate the solution

In this task, you log back into the TestInstance to test that the network firewall properly blocks attempts to access the malicious website files.

30. In the AWS Management Console, enter **EC2** in the search bar, and then choose **EC2**.
31. In the left navigation pane, choose **Instances**.
32. Select the check box next for **TestInstance**, and then choose **Connect**.
33. Choose the **Session Manager** tab, and then choose **Connect**.
34. To change directories and view the current working directory, run the following commands:

```
cd ~
pwd
```

35. To try and access the first malicious file, run the following **wget** command.

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

The output should display the following:

```
HTTP request sent, awaiting response...
```

This output shows that the malware site and file are no longer accessible and have been successfully blocked by the network firewall.

36. Press Ctrl+c to stop the command.
37. To test access to the other malicious URL, run the following command:

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

The output should display the following:

```
HTTP request sent, awaiting response...
```

38. Next, to remove the test malware files, run the following command:

```
rm java_jre17_exec.html js_crypto_miner.html
```

39. To confirm that the files were deleted, run the **ls** command:

```
ls
```

You should see a blank output, which confirms that the files have been removed.

Summary of task 5

In this task, you verified that the network firewall has been updated and configured properly to block the malicious websites. You confirmed that access is blocked by logging into the TestInstance EC2 instance and running **wget** commands to these files. Users are now unable to access these malicious files from this website.

Conclusion

Congratulations! You now have successfully:

- Updated a network firewall
- Created a firewall rules group
- Verified and tested that access to malicious sites is blocked

Lab complete

40. Choose **End Lab** at the top of this page, and then choose **Yes** to confirm that you want to end the lab.
41. An **Ended AWS Lab Successfully** message is briefly displayed indicating that the lab has ended.

For more information about AWS Training and Certification, see AWS Training and Certification.

Your feedback is welcome and appreciated.

If you would like to share any suggestions or corrections, please provide the details in our AWS Training and Certification Contact Form.