Firepower Threat Defense Virtual 구축

이 장에서는 AWS 포털에서 Firepower Threat Defense Virtual를 구축하는 방법을 설명합니다.

Firepower Threat Defense Virtual 인스턴스 구축

Before you begin

다음 작업을 수행하는 것이 좋습니다.

- AWS 환경 구성의 설명에 따라 AWS VPC 및 EC2 요소를 구성합니다.
- Firepower Threat Defense Virtual 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

Procedure

단계 **1** https://aws.amazon.com/marketplace(Amazon Marketplace)로 이동하여 로그인합니다.

단계 **2** Amazon Marketplace에 로그인한 후 Firepower Threat Defense Virtual(NGFWv (Cisco Firepower NGFW Virtual)-BYOL)에 대해 제공된 링크를 클릭합니다.

Note 이전에 AWS를 사용했다면 로그아웃했다가 다시 로그인해야 링크가 작동합니다.

단계 **3** **Continue(**계속**)**를 클릭하고 **Manual Launch(**수동 실행**)** 탭을 클릭합니다.

단계 **4** **Accept Terms(**약관 동의**)**를 클릭합니다.

단계 **5** 원하는 지역에서 **Launch with EC2 Console(EC2** 콘솔로 실행**)**을 클릭합니다.

단계 **6** Firepower Threat Defense Virtual에서 지원하는 **Instance Type**(인스턴스 유형)(c4.xlarge 권장)을 선택합니다.

단계 **7** 화면 하단의 **Next: Configure Instance Details(**다음**:** 인스턴스 상세 정보 구성**)** 버튼을 클릭합니다.

- 이전에 생성한 VPC와 일치하도록 **Network(**네트워크**)**를 변경합니다.
- 이전에 생성한 관리 서브넷과 일치하도록 **Subnet(**서브넷**)**을 변경합니다. IP 주소를 지정하거나 자동 생성을 사용할 수 있습니다.

- 네트워크 인터페이스 아래에서 **Add Device(**디바이스 추가**)** 버튼을 클릭하여 eth1 네트워크 인터페이스를 추가합니다.
- eth0에 사용하기 위해서 이전에 생성한 관리 서브넷과 일치하도록 **Subnet(**서브넷**)**을 변경합니다.

Note Firepower Threat Defense Virtual에는 2개의 관리 인터페이스가 필요합니다.

- **Advanced Details(**고급 상세 정보**)**에서 기본 로그인 정보를 추가합니다. 디바이스 이름과 비밀번호에 대한 요구 사항을 충족하도록 아래의 예시를 수정합니다.

주의**: Advanced Details(**고급 상세 정보**)** 필드에 데이터를 입력할 때는 일반 텍스트만 사용하십시오. 텍스트 편집기에서 이 정보를 복사하는 경우에는 일반 텍스트로만 복사해야 합니다. 유니코드 데이터(공백 포함)를 **Advanced Details(**고급 상세정보**)** 필드에 복사하는 경우, 인스턴스가 손상될 수 있으며 인스턴스를 종료하고 다시 생성해야 합니다.

Firepower Management Center를 사용하여 FTDv를 관리하기 위한 샘플 로그인 컨피그레이션:

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<Your_hostname>",
            "ManageLocally": "No",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>",
}
```

Firepower Device Manager를 사용하여 FTDv를 관리하기 위한 샘플 로그인 컨피그레이션:

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<Your_hostname>",
            "ManageLocally": "Yes",
}
```

단계 **8** **Next: Add Storage(**다음**:** 스토리지 추가**)**를 클릭합니다.

기본값을 수락하거나 볼륨을 변경할 수 있습니다.

단계 **9** **Next: Tag Instance(**다음**:** 인스턴스 태그 지정**)**를 클릭합니다.

태그는 대/소문자를 구별하는 키-값 쌍으로 구성됩니다. 예를 들어 **Key(**키**)** = Name, **Value(**값**)** = Firewall을 사용하여 태그를 정의할 수 있습니다.

단계 **10** **Next: Configure Security Group(**다음**:** 보안 그룹 구성**)**을 선택합니다.

단계 **11** **Select an existing Security Group(**기존 보안 그룹 선택**)**을 클릭하고 이전에 구성한 보안 그룹을 선택하거나 새 보안 그룹을 생성합니다. 보안 그룹 생성에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

단계 **12** **Review and Launch(**검토 및 실행**)**를 클릭합니다.

단계 **13** **Launch(**실행**)**를 클릭합니다.

단계 **14** 기존 키 쌍을 선택하거나 새 키 쌍을 생성합니다.

Note 기존 키 쌍을 선택하거나 새 키 쌍을 생성할 수 있습니다. 키 쌍은 AWS가 저장하는 공개 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 키 쌍은 인스턴스에 연결하는 데 필요할 수도 있으므로 확인된 위치에 저장해야 합니다.

단계 **15** **Launch Instances(**인스턴스 실행**)**를 클릭합니다.

단계 **16** **View Launch(**보기 실행**)**를 클릭하고 프롬프트를 따릅니다.

단계 **17** **EC2 Dashboard(EC2** 대시보드**) > Network Interfaces(**네트워크 인터페이스**)**를 클릭합니다**.**

단계 **18** AWS 환경 구성에서 이전에 생성한 트래픽 인터페이스를 찾은 다음 **Attach(**연결**)**를 클릭합니다. 이는 Firepower Threat Defense Virtual 인스턴스에서 **eth2** 인터페이스가 됩니다.

단계 **19** AWS 환경 구성에서 이전에 생성한 트래픽 인터페이스를 찾은 다음 **Attach(**연결**)**를 클릭합니다. 이는 Firepower Threat Defense Virtual 인스턴스에서 **eth3** 인터페이스가 됩니다.

Note 4개의 인터페이스를 구성해야 합니다. 그렇지 않으면 Firepower Threat Defense Virtual에서 부팅 프로세스를 완료하지 않습니다.

단계 **20** **EC2 Dashboard(EC2** 대시보드**) > Instances(**인스턴스**)**를 클릭합니다.

단계 **21** 상태를 보려면 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Instance Settings(**인스턴스 설정**) > Get System Log(**인스턴스 시스템 로그**)**를 선택합니다.

Note 연결 문제에 대한 경고가 있을 수 있습니다. 이는 EULA가 완료될 때까지 eth0 인터페이스가 활성화되지 않기 때문입니다.

단계 **22** 20분 후에 Firepower Threat Defense Virtual을 Firepower Management Center에 등록할 수 있습니다.

What to do next

다음 단계는 선택한 관리 모드에 따라 달라집니다.

- **Enable Local Manager(**로컬 매니저 활성화**)**에 대해 **No(**아니요**)**를 선택한 경우 Firepower Management Center을 사용해 FTDv를 관리할 수 있습니다. Firepower Management Center로 Firepower Threat Defense Virtual 관리를 참조하십시오.
- **Enable Local Manager(**로컬 매니저 활성화**)**에 대해 **Yes(**예**)**를 선택한 경우 Firepower Device Manager을 사용해 FTDv를 관리할 수 있습니다. Firepower Device Manager를 이용한 Firepower Threat Defense Virtual 관리를 참조하십시오.

관리 옵션을 선택하는 방법에 대한 개요는 Firepower 디바이스 관리 방법을 참조하십시오.