GCP에서 Firepower Threat Defense Virtual 구축

Google에서 제공하는 고 가용성 호스팅 환경에서 애플리케이션을 실행할 수 있는 퍼블릭 클라우드 컴퓨팅 서비스인 Google Cloud Platform(GCP)에 FTDv를 구축 할 수 있습니다.

GCP 콘솔 **Dashboard(**대시 보드**)**에 GCP 프로젝트 정보가 표시됩니다.

- 아직 선택하지 않은 경우 **Dashboard(**대시 보드**)**에서 GCP 프로젝트를 선택해야 합니다.
- Dashboard(대시 보드)에 액세스하려면 **Navigation(**탐색**)** 메뉴 > **Home(**홈**)** > **Dashboard(**대시 보드**)**를 클릭합니다.

GCP 콘솔에 로그인하여 GCP Marketplace에서 Cisco Firepower NGFW virtual firewall(NGFWv) 제품을 검색한 다음 FTDv 인스턴스를 시작합니다. 다음 절차에서는 GCP 환경을 준비하고 FTDv 인스턴스를 시작하여 FTDv를 구축하는 방법을 설명합니다.

- VPC 네트워크 생성, 1 페이지
- 방화벽 규칙 생성, 2 페이지
- GCP에서 FTDv 인스턴스 생성, 3 페이지

VPC 네트워크 생성

FTDv를 구축하려면 FTDv를 구축하기 전에 4개의 네트워크를 생성해야 합니다. 네트워크는 다음과 같습니다.

- 관리 서브넷의 관리 VPC
- 진단 VPC 또는 진단 서브넷
- 내부 서브넷의 내부 VPC
- 외부 서브넷의 외부 VPC

또한 FTDv로 트래픽 흐름을 허용하도록 경로 테이블 및 GCP 방화벽 규칙을 설정합니다. 경로 테이블 및 방화벽 규칙은 FTDv 자체에 구성된 규칙과 다릅니다. 연결된 네트워크 및 기능에 따라 GCP 경로 테이블 및 방화벽 규칙의 이름을 지정합니다. GCP에서 FTDv를 위한 네트워크 토폴로지 샘플을 지침으로 참고합니다.

프로시저

단계 **1** GCP 콘솔에서 **VPC networks(VPC** 네트워크**)**를 선택하고 **Create VPC Network(VPC** 네트워크 생성**)**를 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 원하는 이름을 입력합니다.

단계 **3** **Subnet creation mode(**서브넷 생성 모드**)**에서 **Custom(**맞춤형**)**을 클릭합니다.

단계 **4** **New subnet(**새로운 서브넷**)** 아래의 **Name(**이름**)** 필드에 원하는 이름을 입력합니다.

단계 **5** **Region(**지역**)** 드롭 다운 목록에서 자신의 구축에 적합한 지역을 선택합니다. 네 개의 네트워크는 모두 같은 지역에 있어야 합니다.

단계 **6** **IP address range(IP** 주소 지역**)** 필드에 CIDR 포맷, 예를 들면 10.10.0.0/24의 형식으로 첫 번째 네트워크의 서브넷을 입력합니다.

단계 **7** 기타 모든 설정은 기본값으로 하고 **Create(**생성**)**를 클릭합니다.

단계 **8** 나머지 3 개의 VPC 네트워크를 생성하려면 1 ~ 7 단계를 반복합니다.

방화벽 규칙 생성

FTDv 인스턴스를 구축하는 동안 관리 인터페이스에 대한 방화벽 규칙을 적용합니다(SSH 및 SFTunnel이 FMC와 통신할 수 있도록). GCP에서 FTDv 인스턴스 생성, 3 페이지을 참조하십시오. 요구 사항에 따라 내부, 외부 및 진단 인터페이스에 대한 방화벽 규칙을 생성 할 수도 있습니다.

프로시저

단계 **1** GCP 콘솔에서 **Networking(**네트워킹**)** > **VPC network(VPC** 네트워크**)** > **Firewall(**방화벽**)**을 선택하고 **Create Firewall Rule(**방화벽 규칙 생성**)**을 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 방화벽 규칙을 설명하는 이름(예: *vpc-asiasouth-inside-fwrule*)을 입력합니다.

단계 **3** **Network(**네트워크**)** 드롭 다운 목록에서 방화벽 규칙을 생성할 VPC 네트워크의 이름(예: *ftdv-south-inside*)을 선택합니다.

단계 **4** **Targets(**대상**)** 드롭 다운 목록에서 방화벽 규칙을 위해서 적용할 옵션(예: **All instances in the network**)을 선택합니다.

단계 **5** **Source IP(**소스 **IP)** 범위 필드에서 CIDR 형식(예: 0.0.0.0/0)으로 소스 IP 주소 범위를 입력합니다.

트래픽은 이들 IP 주소 범위 내의 소스로부터만 허용됩니다.

단계 **6** **Protocols and ports(**프로토콜 및 포트**)** 아래에서 **Specified protocols and ports(**명시된 프로토콜 및 포트**)**를 선택합니다.

단계 **7** 보안 규칙을 추가합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

GCP에서 FTDv 인스턴스 생성

아래 단계에 따라 GCP Marketplace에서 Cisco Firepower NGFW Virtual Firewall(NGFWv) 제품을 사용하여 FTDv 인스턴스를 구축할 수 있습니다.

프로시저

단계 **1** GCP 콘솔로 로그인합니다.

단계 **2** **Navigation(**탐색**)** 메뉴**(** > **Marketplace(**마켓플레이스**)**를 클릭합니다 .

단계 **3** Marketplace에서 "Cisco Firepower NGFW Virtual Firewall (NGFWv)"을 검색하고 제품을 선택합니다.

단계 **4** **Launch(**실행**)**를 클릭합니다.

a) **Deployment name(**구축 이름**)** — 인스턴스를 위한 고유한 이름을 지정합니다.

b) **Zone(**영역**)** — FTDv를 구축하고자 하는 영역을 선택합니다.

c) **Machine type(**시스템 유형**)** — GCP 시스템 유형 지원에 따라 정확한 시스템 유형을 선택합니다.

d) **SSH key (SSH** 키**)(**선택**)** — SSH 키 쌍의 공용 키를 붙여넣기합니다.

키 쌍은 GCP가 저장하는 공용 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 인스턴스에 연결할 때 필요한 만큼 키 쌍을 알고 있는 위치에 확실히 저장해야 합니다.

e) 이 인스턴스에 액세스하기 위해 프로젝트 전체 SSH 키를 허용할지 아니면 차단할지를 선택합니다. Google 문서 Allowing or blocking project-wide public SSH keys from a Linux instance를 참조하십시오.

f) 시작 스크립트 - 인스턴스가 부팅될 때마다 자동화된 작업을 수행하도록 FTDv 인스턴스에 대한 시작 스크립트를 생성할 수 있습니다.

다음 예는 시작 스크립트 필드에 복사하여 붙여 넣은 Day0 컨피그레이션의 샘플을 보여줍니다.

```
{
"AdminPassword": "Cisco@123123",
"Hostname": "ftdv-gcp",
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

팁 실행 오류를 방지하려면 JSON 검사기를 사용하여 Day0 컨피그레이션을 검증해야 합니다.

g) 네트워크 인터페이스 - 인터페이스 구성: 1) 관리, 2) 진단, 3) 내부, 4) 외부.

참고 인터페이스를 생성한 후엔 거기에 인터페이스를 추가할 수 없습니다. 부적절한 인터페이스 컨피그레이션으로 인스턴스를 생성했을 경우 해당 인스턴스를 삭제하고 적절한 인터페이스 컨피그레이션으로 다시 생성해야 합니다.

1. **Network(**네트워크**)** 드롭 다운 목록에서 VPC 네트워크(예 : *vpc-asiasouth-mgmt*)를 선택합니다.
2. **External IP(**외부 **IP)** 드롭 다운 목록에서 적절한 옵션을 선택합니다.

   관리 인터페이스를 위해선 **External IP(**외부 **IP) - Ephemeral(**일회성**)**을 선택합니다. 이는 내부 및 외부 인터페이스의 경우 선택 사항입니다.
3. **Done(**완료**)**을 클릭합니다.

h) **Firewall(**방화벽**)**— 방화벽 규칙을 적용합니다.

- 인터넷의 **TCP** 포트 **22** 트래픽**(SSH** 액세스**)** 허용 확인란을 선택하여 SSH를 허용합니다.
- 인터넷의 **HTTPS** 트래픽**(FMC** 액세스**)** 허용 확인란을 선택하여 FMC를 허용하고 양방향, SSL 암호화 통신 채널(SFTunnel)을 사용하여 관리되는 디바이스가 통신할 수 있도록 합니다.

i) **More(**더 보기**)**를 클릭하여 보기를 확장하고 **IP Forwarding(IP** 전달**)**이 **On(**켜짐**)**으로 설정되어 있는지 확인합니다.

단계 **5** **Deploy(**구축**)**를 클릭합니다.

GCP 콘솔의 VM 인스턴스 페이지에서 인스턴스 상세 정보를 확인합니다. 내부 IP 주소, 외부 IP 주소 그리고 인스턴스를 시작하고 중지할 수 있는 제어 기능을 확인할 수 있습니다. 인스턴스를 수정해야 하는 경우 인스턴스를 중지해야 합니다.