Firepower Threat Defense Virtual 및 Google Cloud Platform 시작하기

Firepower Threat Defense Virtual(FTDv)는 Cisco의 Firepower 차세대 방화벽 기능을 가상화된 환경으로 가져와 일관된 보안 정책으로 물리, 가상 및 클라우드 환경 전반 및 클라우드 간 워크로드를 준수하도록 합니다.

이 장에서는 기능 지원, 시스템 요구 사항, 지침, 제한 사항 등 Google Cloud Platform(GCP) 환경 내에서의 Firepower Threat Defense Virtual 기능에 대해 설명합니다. 이 장에서는 FTDv을(를) 관리하기 위한 옵션에 대해서도 설명합니다.

구축을 시작하기 전에 관리 옵션을 이해하는 것이 중요합니다. Firepower Management Center를 사용하여 FTDv을 관리하고 모니터링할 수 있습니다.

GCP에서 FTDv 구축

Firepower Threat Defense Virtual(FTDv)은 물리적 Cisco FTD와 동일한 소프트웨어를 실행하여 가상 폼 팩터에서 검증된 보안 기능을 제공합니다. FTDv은 퍼블릭 GCP에서 구축될 수 있습니다. 그러면 시간이 경과함에 따라 해당 위치를 확장, 축소 또는 이동하는 가상 및 물리적 데이터 센터 워크로드를 보호하기 위한 구성이 가능하게 됩니다.

GCP 시스템 유형 지원

FTDv 필요에 따라 Google 가상 머신 유형 및 크기를 선택합니다. 현재 FTDv은 컴퓨팅 최적화 및 범용 시스템(표준, 고용량 메모리 그리고 고 CPU 시스템 유형)을 모두 지원합니다.

참고 지원되는 시스템 유형은 예고 없이 변경될 수 있습니다.

표 *1:* 지원되는 컴퓨팅 최적화 시스템 유형

컴퓨팅 최적화 시스템 유형	속성	
	vCPUs	**RAM(GB)**
c2-standard-4	4	16GB
c2-standard-8	8	32GB
c2-standard-16	16	64GB

표 *2:* 지원되는 범용 시스템 유형

범용 시스템 유형	속성	
	vCPUs	**RAM(GB)**
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-8	8	7.2
n1-highcpu-16	16	14.4
n2-highcpu-8	8	8
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- FTDv에는 최소 4 개의 인터페이스가 필요합니다.
- 지원되는 최대 vCPU는 16개입니다.

GCP에서 계정을 생성하고, GCP Marketplace의 Cisco Firepower NGFW virtual firewall(NGFWv) 제품을 사용해서 VM 인스턴스를 실행한 다음 GCP 시스템 유형을 선택합니다.

FTDv 및 GCP의 사전 요건

- https://cloud.google.com에서 GCP 계정을 생성합니다.

- GCP 프로젝트를 생성합니다. Google 문서, 프로젝트 생성을 참조하십시오.
- Cisco Smart Account는 Cisco Software Central(https://software.cisco.com/)에서 생성할 수 있습니다.
- Firepower Threat Defense Virtual에 라이선스를 부여합니다.
  - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 구성 가이드의 *Firepower System* 라이선싱을 참조하십시오.
- 인터페이스 요구 사항:
  - 관리 인터페이스(2) - Firepower Threat Defense Virtual를 Firepower Management Center에 연결하는 데 사용되는 인터페이스, 진단에 사용되는 인터페이스는 통과 트래픽에는 사용할 수 없습니다.
  - 트래픽 인터페이스(2) - Firepower Threat Defense Virtual를 내부 호스트 및 공용 네트워크에 연결하는 데 사용됩니다.
- 통신 경로:
  - Firepower Threat Defense Virtual에 액세스하기 위한 공용 IP.
- FTDv 시스템 요구 사항은 Cisco FirePOWER 호환성 가이드를 참조하십시오.

FTDv 및 GCP의 지침 및 제한 사항

지원 기능

- GCP 컴퓨팅 엔진에서 구축
- 인스턴스당 최대 16개의 vCPU
- 라우팅 모드(기본값)
- 라이선싱 – BYOL만 지원됩니다.

지원되지 않는 기능

- IPv6
- FTDv 기본 HA
- 자동 확장
- 투명/인라인/패시브 모드
- 점보 프레임

GCP에서 FTDv를 위한 네트워크 토폴로지 샘플

다음 그림은 Routed Firewall Mode의 FTDv에 대한 권장 토폴로지와 FTDv에 대해서 GCP에 구성된 4개의 서브넷(관리, 진단, 내부 및 외부)을 보여줍니다.

그림 *1: GCP* 구축에 대한 *FTDv* 샘플