Secure Firewall Threat Defense Virtual 및 OpenStack으로 시작하기

OpenStack 환경의 컴퓨팅 노드에서 실행 중인 KVM(Kernel-based Virtual Machine) 하이퍼바이저에 Secure Firewall Threat Defense Virtual(이전 Firepower Threat Defense Virtual) 을 구축할 수 있습니다.

OpenStack에서의 Threat Defense Virtual 구축 정보

이 가이드에서는 OpenStack 환경에서 threat defense virtual를 구축하는 방법을 설명합니다. OpenStack은 무료 개방형 표준 클라우드 컴퓨팅 플랫폼으로, 가상 서버 및 기타 리소스가 사용자에게 제공되는 퍼블릭 및 프라이빗 클라우드 모두에서 대부분 IaaS(infrastructure-as-a-service)로 구축됩니다.

이 구축에서는 KVM 하이퍼바이저를 사용하여 가상 리소스를 관리합니다. KVM은 가상화 확장 프로그램(예: Intel VT)이 포함된 x86 하드웨어의 Linux용 전체 가상화 솔루션입니다. KVM은 로드 가능한 커널 모듈인 kvm.ko로 구성되어 있으며, 코어 가상화 인프라 및 kvm-intel.ko와 같은 프로세서별 모듈을 제공합니다.

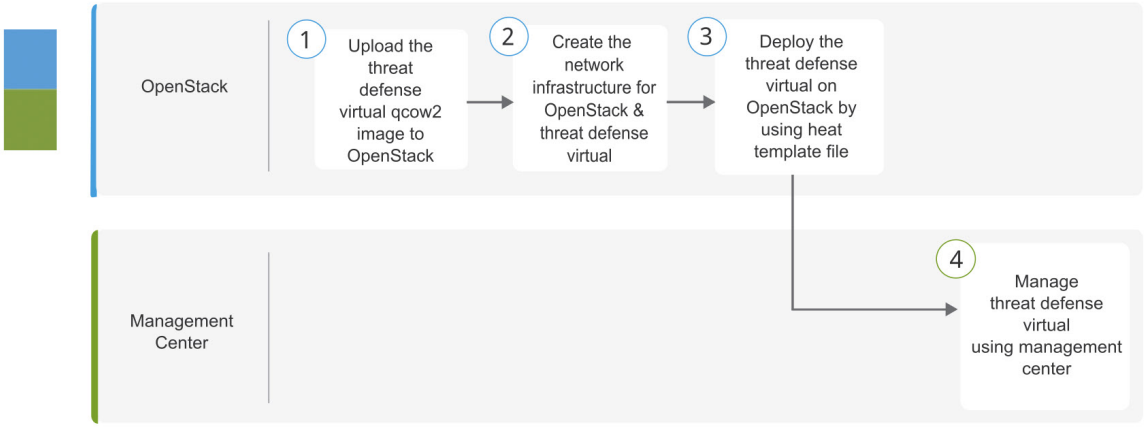
KVM을 사용하여 수정되지 않은 OS 이미지를 실행하는 여러 가상 머신을 실행할 수 있습니다. 각 가상 머신에는 네트워크 카드, 디스크, 그래픽 어댑터 등의 개인 가상화 하드웨어가 있습니다.

디바이스는 KVM 하이퍼바이저에서 이미 지원되므로 OpenStack 지원을 활성화하는 데 추가 커널 패키지 또는 드라이버가 필요하지 않습니다.

참고 OpenStack의 Threat Defense Virtual은 모든 최적화된 다중 노드 환경에 설치할 수 있습니다.

엔드 투 엔드 절차

다음 순서도는 OpenStack에서 Threat Defense Virtual을 구축하기 위한 워크플로를 보여줍니다.



	Workspace	단계
1	OpenStack	OpenStack에 Threat Defense Virtual 구축: Threat Defense Virtual 이미지를 OpenStack에 업로드합니다.
2	OpenStack	OpenStack에 Threat Defense Virtual 구축: OpenStack 및 Threat Defense Virtual용 네트워크 인프라를 생성합니다.
3	OpenStack	OpenStack에 Threat Defense Virtual 구축: Threat Defense Virtual 히트 템플릿 파일을 사용해 OpenStack에 Threat Defense Virtual을 구축합니다.
4	Management Center	Threat Defense Virtual 관리: • Management Center 사용

Threat Defense Virtual 및 OpenStack에 대한 사전 요건

- software.cisco.com에서 qcow2 threat defense virtual 이미지를 가져옵니다.
- Threat Defense Virtual은 오픈 소스 OpenStack 환경 및 Cisco VIM 관리 OpenStack 환경에서의 구축을 지원합니다.

  OpenStack 지침에 따라 OpenStack 환경을 설정합니다.

  - 오픈 소스 OpenStack 문서를 참조하십시오.

    Stein 릴리스 - https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html

Queens 릴리스 - https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/overview.html

- Cisco VIM(Virtualized Infrastructure Manager) OpenStack 문서: Cisco Virtualized Infrastructure Manager 설명서, 3.4.3~3.4.5를 참조하십시오.

- Cisco Smart Account는 Cisco Software Central에서 생성할 수 있습니다.
- threat defense virtual에 라이선스를 부여합니다.
  - management center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스 관리 방법에 대한 자세한 내용은 *Secure Firewall Management Center* 관리 가이드의 "라이선싱"을 참조하십시오.
- 인터페이스 요구 사항:
  - 관리 인터페이스(2) - threat defense virtual를 management center에 연결하는 데 사용되는 인터페이스, 진단에 사용되는 인터페이스는 통과 트래픽에는 사용할 수 없습니다.
  - 내부 및 외부 인터페이스 - threat defense virtual를 내부 호스트 및 공용 네트워크에 연결하는 데 사용됩니다.
- 통신 경로:
  - threat defense virtual에 액세스하기 위한 부동 IP.
- 최소 지원되는 threat defense virtual 버전:
  - 버전 7.0
- OpenStack 요구 사항은구축을 위한 OpenStack 요구 사항, 5 페이지 를 참조하십시오.
- threat defense virtual 시스템 요구 사항은 Cisco Firepower 호환성을 참조하십시오.

Threat Defense Virtual 및 OpenStack에 대한 지침 및 제한 사항

지원 기능

OpenStack의 threat defense virtual는 다음 기능을 지원합니다.

- OpenStack 환경의 컴퓨팅 노드에서 실행 중인 KVM 하이퍼바이저의 threat defense virtual 구축.
- OpenStack CLI
- Heat 템플릿 기반 구축
- OpenStack Horizon 대시보드

- 라우팅 모드(기본값)
- 라이선싱 – BYOL만 지원됩니다.
- management center를 사용해 Threat Defense Virtual 관리
- 드라이버 - virtIO, VPP 및 SR-IOV

Threat Defense Virtual 스마트 라이선싱의 성능 계층

threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.

표 *1:* 자격 기준 ***Threat Defense Virtual*** 라이선스 기능 제한

성능 계층	디바이스 사양 **(Core/RAM)**	속도 제한	**RA VPN** 세션 제한
FTDv5	4 코어/8GB	100Mbps	50
FTDv10	4 코어/8GB	1Gbps	250
FTDv20	4 코어/8GB	3Gbps	250
FTDv30	8 코어/16GB	5Gbps	250
FTDv50	12 코어/24GB	10Gbps	750
FTDv100	16 코어/32GB	16Gbps	10,000

threat defense virtual 디바이스 라이선싱에 대한 지침은 *Secure Firewall Management Center* 관리자 가이드의 "라이선싱" 장을 참조하십시오.

성능 최적화

threat defense virtual에서 최상의 성능을 얻으려면 VM과 호스트를 모두 조정할 수 있습니다. 자세한 내용은 OpenStack의 가상화 조정 및 최적화를 참조하십시오.

Receive Side Scaling— threat defense virtual는 RSS(Receive Side Scaling)를 지원합니다. RSS는 네트워크 수신 트래픽을 여러 프로세서 코어로 분산하기 위해 네트워크 어댑터에서 활용하는 기술입니다. 버전 7.0 이상에서 지원됩니다. 자세한 내용은 RSS(Receive Side Scaling)를 위한 다중 RX 대기열을 참조하십시오.

Snort

- Snort를 종료하는 데 시간이 오래 걸리거나, VM이 일반적으로 느려지거나, 특정 프로세스가 실행되는 등의 비정상적인 동작이 관찰되는 경우 threat defense virtual 및 VM 호스트에서 로그를 수집합니다. 전체 CPU 사용량, 메모리, I/O 사용량 및 읽기/쓰기 속도 로그를 수집하면 문제를 해결하는 데 도움이 됩니다.

- Snort가 종료될 때 높은 CPU 및 I/O 사용량이 관찰됩니다. 메모리가 충분하지 않고 전용 CPU가 없는 단일 호스트에서 여러 threat defense virtual 인스턴스가 생성된 경우 Snort가 종료되는 데 시간이 오래 걸리므로 Snort 코어가 생성됩니다.

지원되지 않는 기능

OpenStack의 threat defense virtual는 다음을 지원하지 않습니다.

- 자동 확장
- OpenStack Stein 및 Queens 릴리스 이외의 OpenStack 릴리스
- Ubuntu 18.04 버전 및 RHEL(Red Hat Enterprise Linux) 7.6 이외의 운영 체제

구축을 위한 OpenStack 요구 사항

OpenStack 환경은 다음의 지원되는 하드웨어 및 소프트웨어 요구 사항을 준수해야 합니다.

표 *2:* 하드웨어 및 소프트웨어 요건

카테고리	지원되는 버전	**Notes(참고)**
서버 하드웨어	UCS C240 M5	os-controller 및 os-compute 노드에 대해 각각 하나씩, 2개의 UCS 서버가 권장됩니다.
동인	VIRTIO, IXGBE, I40E	다음은 지원되는 드라이버입니다.
운영 체제	Ubuntu Server 18.04	이는 UCS 서버의 권장 OS입니다.
OpenStack 버전	Stein 릴리스	다양한 OpenStack 릴리스에 대한 세부 정보는 다음에서 확인할 수 있습니다. https://releases.openstack.org/

표 *3: Cisco VIM Managed OpenStack*의 하드웨어 및 소프트웨어 요구 사항

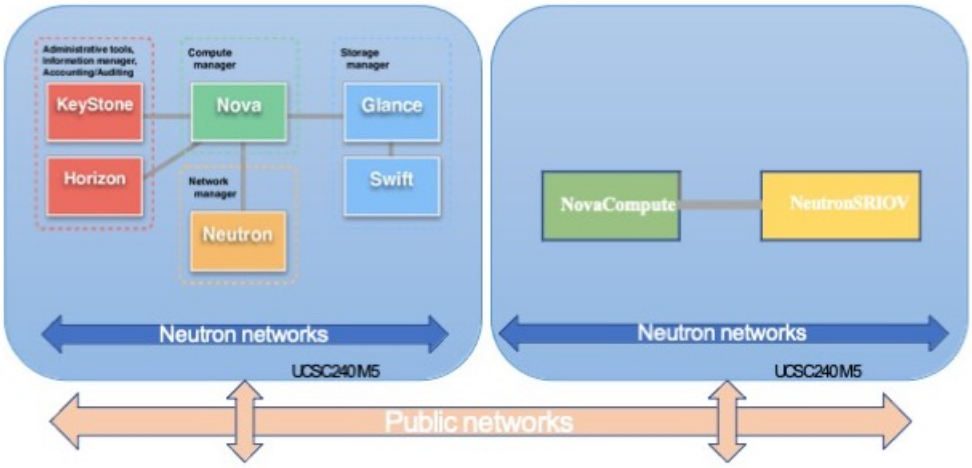
카테고리	지원되는 버전	**Notes(참고)**
서버 하드웨어	UCS C220-M5/UCS C240-M4	5개의 UCS 서버를 사용하는 것이 좋습니다. os-controller에는 각각 3개, os-compute 노드에는 2개 이상입니다.

카테고리	지원되는 버전	Notes(참고)
동인	VIRTIO, SRIOV 및 VPP	다음은 지원되는 드라이버입니다.
운영 체제	Red Hat Enterprise Linux 7.6	권장되는 OS입니다.
OpenStack 버전	OpenStack 13.0(Queens 릴리스)	다양한 OpenStack 릴리스에 대한 세부 정보는 다음에서 확인할 수 있습니다. https://releases.openstack.org/
Cisco VIM 버전	Cisco VIM 3.4.4	Cisco VIM OpenStack 문서를 참고하십시오.https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/cvim/3_4_3_to_3_4_5/Cisco_Virtual_Infrastructure_Manager_Documentation_3_4_3_to_3_4_5.pdf

OpenStack 플랫폼 토폴로지

다음 그림에는 2개의 UCS 서버를 사용하여 OpenStack에서 구축을 지원하기 위한 권장 토폴로지가 나와 있습니다.

그림 *1: OpenStack* 플랫폼 토폴로지



OpenStack의 Threat Defense Virtual에 대한 네트워크 토폴로지 예

다음 그림은 Routed Firewall Mode의 threat defense virtual에 대한 예시 네트워크 토폴로지와 threat defense virtual에 대해서 OpenStack에 구성된 4개의 서브넷(관리, 진단, 내부 및 외부)을 보여줍니다.

그림 *2: Threat Defense Virtual* 및 *OpenStack*의 *Management Center Virtual*에 대한 토폴로지 예