Deploy the Threat Defense Virtual on OpenStack

Overview

This guide describes how to deploy the threat defense virtual in an OpenStack environment. OpenStack is a free open standard cloud computing platform, mostly deployed as infrastructure-as-a-service (IaaS) in both public and private clouds where virtual servers and other resources are made available to users.

This deployment uses a KVM hypervisor to manage virtual resources. KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko.

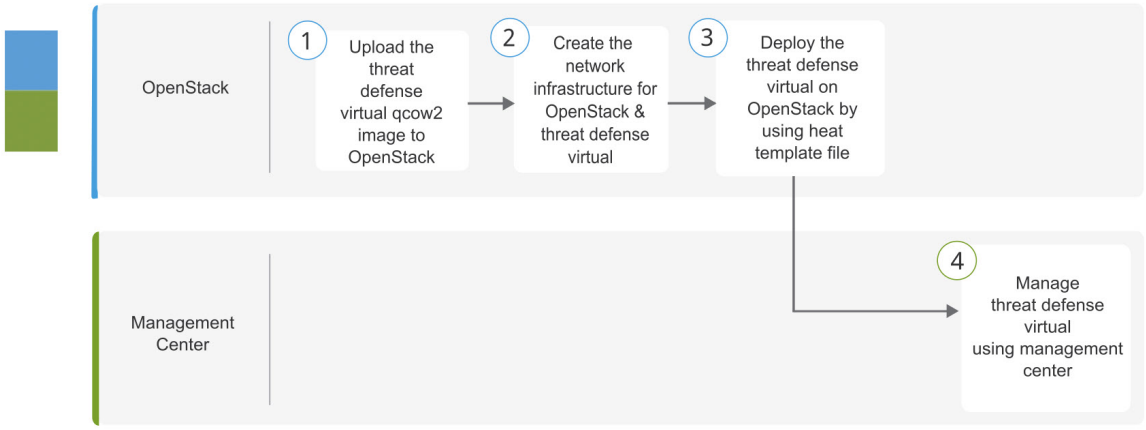
You can run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

Because devices are already supported on the KVM hypervisor, no additional kernel packages or drivers are needed to enable OpenStack support.

Note Threat Defense Virtual on OpenStack can be installed on any optimized multi-node environment.

End-to-End Procedure

The following flowchart illustrates the workflow for deploying threat defense virtual on OpenStack.



	Workspace	Steps
1	OpenStack	Upload the Threat Defense Virtual Image to OpenStack: Upload the threat defense virtual image to OpenStack.
2	OpenStack	Create the Network Infrastructure for OpenStack and Threat Defense Virtual: Create the network infrastructure for OpenStack and threat defense virtual.
3	OpenStack	Deploy the Threat Defense Virtual on OpenStack: Deploy the threat defense virtual on OpenStack by using threat defense virtual heat template file.
4	Management Center	Manage the threat defense virtual by using the Management Center

Prerequisites

- Get the qcow2 threat defense virtual image from software.cisco.com.
- Threat Defense Virtual supports deployment on opensource OpenStack environment and Cisco VIM managed OpenStack environment.

  Set up the OpenStack environment according to the OpenStack guidelines.

  - See the opensource OpenStack document:

    Wallaby Release - https://docs.openstack.org/project-deploy-guide/openstack-ansible/wallaby/overview.html

  - See the Cisco Virtualized Infrastructure Manager (VIM) OpenStack document: Cisco Virtualized Infrastructure Manager Documentation, 4.4.3.

- A Cisco Smart Account. You can create one at Cisco Software Central.
- License the threat defense virtual.
  - Configure all license entitlements for the security services from the management center.

    - See “Licensing” in the *Secure Firewall Management Center Admin Guide* for more information about how to manage licenses.

- Interface requirements:
    - Management interfaces (2) — One used to connect the threat defense virtual to the management center, second used for diagnostics; cannot be used for through traffic.
    - Inside and outside interfaces — Used to connect the threat defense virtual to inside hosts and to the public network.
- Communications paths:
    - Floating IPs for access into the threat defense virtual.
- Minimum supported the threat defense virtual version:
    - Version 7.0
- For OpenStack requirements, see System Requirements, on page 4.
- For threat defense virtual system requirements, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

Supported Features

The threat defense virtual on OpenStack supports the following features:

- Deployment of threat defense virtual on the KVM hypervisor running on a compute node in your OpenStack environment.
- OpenStack CLI
- Heat template-based deployment
- OpenStack Horizon dashboard
- IPv6
- Licensing – Only BYOL is supported
- Threat Defense Virtual management using the management center only.
- Drivers - virtIO and SR-IOV

Performance Tiers for Threat Defense Virtual Smart Licensing

The threat defense virtual supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements.

Table 1: Threat Defense Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5	4 core/8 GB	100Mbps	50
FTDv10	4 core/8 GB	1Gbps	250
FTDv20	4 core/8 GB	3Gbps	250
FTDv30	8 core/16 GB	5Gbps	250
FTDv50	12 core/24 GB	10Gbps	750
FTDv100	16 core/32 GB	16Gbps	10,000

See the "Licensing" chapter in the *Secure Firewall Management Center Admin Guide* for guidelines when licensing your threat defense virtual device.

Performance Optimizations

To achieve the best performance out of the threat defense virtual, you can make adjustments to the both the VM and the host. See Virtualization Tuning and Optimization on OpenStack for more information.

Receive Side Scaling—The threat defense virtual supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic to multiple processor cores. Supported on Version 7.0 and later. See Multiple RX Queues for Receive Side Scaling (RSS) for more information.

Snort

- If you are observing abnormal behavior such as Snort taking a long time to shut down, or the VM being slow in general or when a certain process is executed, collect logs from the threat defense virtual and the VM host. Collection of overall CPU usage, memory, I/O usage, and read/write speed logs will help troubleshoot the issues.
- High CPU and I/O usage is observed when Snort is shutting down. If a number of threat defense virtual instances have been created on a single host with insufficient memory and no dedicated CPU, Snort will take a long time to shut down which will result in the creation of Snort cores.

Unsupported Features

The threat defense virtual on OpenStack does not support the following:

- Autoscale
- Cluster

System Requirements

The OpenStack environment must conform to the following supported hardware and software requirements.

Table 2: Hardware and Software Requirements for Open Source OpenStack

Category	Supported Versions	Notes
Server Hardware	UCS C240 M5	2 UCS servers are recommended, one each for os-controller and os-compute nodes.
Drivers	VIRTIO, IXGBE, and I40E	These are the supported drivers.
Operating System	Ubuntu Server 20.04	This is the recommended OS on UCS servers.
OpenStack Version	Wallaby release	Details of the various OpenStack releases are available at: https://releases.openstack.org/

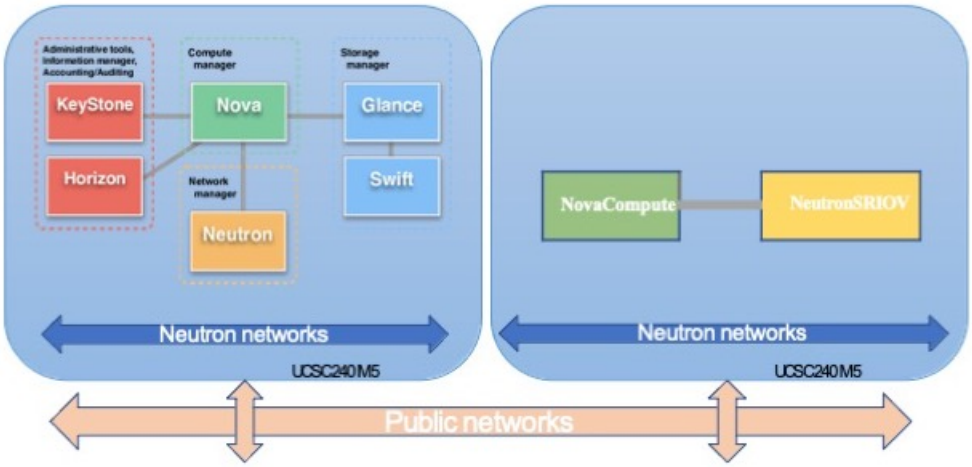
Table 3: Hardware and Software Requirements for Cisco VIM Managed OpenStack

Category	Supported Versions	Notes
Server Hardware	UCS C220-M5/UCS C240-M4	5 UCS servers are recommended, three each for os-controller and Two or more for os-compute nodes.
Drivers	VIRTIO, IXGBE, and I40E	These are the supported drivers.
Cisco VIM Version	Cisco VIM 4.4.3 Supported on: • Operating System - Red Hat Enterprise Linux 8.4 • OpenStack version - OpenStack 16.2 (Train Release)	See Cisco Virtualized Infrastructure Manager Documentation, 4.4.3 for more information.

OpenStack Platform Topology

The following figure shows the recommended topology to support deployments in OpenStack using two UCS servers.

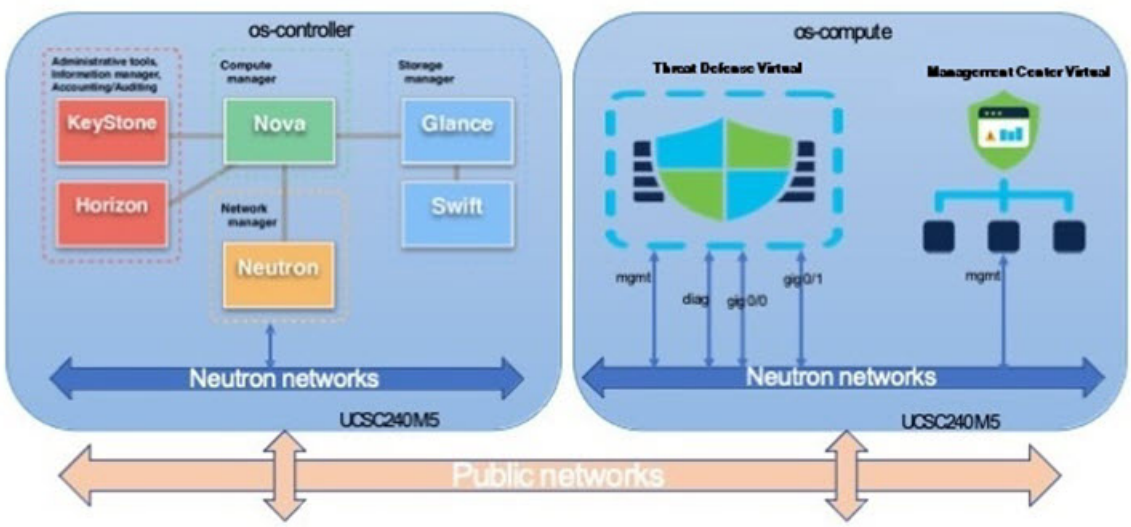
Figure 1: OpenStack Platform Topology



Network Topology Example for Threat Defense Virtual on OpenStack

The following figure shows an example network topology for the threat defense virtual in Routed Firewall Mode with 4 subnets configured in OpenStack for the threat defense virtual (management, diagnostic, inside, and outside).

Figure 2: Topology Example with Threat Defense Virtual and Management Center Virtual on OpenStack



Deploy the Threat Defense Virtual

Cisco provides sample heat templates for deploying the threat defense virtual. Steps for creating the OpenStack infrastructure resources are combined in a heat template (`deploy_os_infra.yaml`) file to create networks, subnets, and router interfaces. At a high-level, the threat defense virtual deployment steps are categorized into the following sections.

- Upload the threat defense virtual qcow2 image to the OpenStack Glance service.
- Create the network infrastructure:
  - Network
  - Subnets
  - Router interface
- Create the threat defense virtual instance:
  - Flavor
  - Security Groups
  - Floating IP
  - Instance

You can deploy the threat defense virtual on OpenStack using the following steps.

Upload the Threat Defense Virtual Image to OpenStack

Copy the threat defense virtual qcow2 image to the OpenStack controller node, and then upload the image to the OpenStack Glance service.

Before you begin

Download the threat defense virtual qcow2 file from Cisco.com and put it on your Linux host:

https://software.cisco.com/download/navigator.html

Note A Cisco.com login and Cisco service contract are required.

Procedure

Step 1 Copy the qcow2 image file to the OpenStack controller node.

Step 2 Upload the threat defense virtual image to the OpenStack Glance service.

```
root@ucs-os-controller:$ openstack image create <image_name> --public --disk-
format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

Step 3 Verify if the threat defense virtual image upload is successful.

root@ucs-os-controller:$ openstack image list

Example:

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+---------+
| ID                                   | Name              | Status |+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image    | active |+
```

The uploaded image and it's status is displayed.

What to do next

Create the network infrastructure using the `deploy_os_infra.yaml` template.

Create the Network Infrastructure for OpenStack and Threat Defense Virtual

Before you begin

Heat template files are required to create the network infrastructure and the required components for threat defense virtual, such as flavor, networks, subnets, router interfaces, and security group rules:

- `deploy_os_infra.yaml`
- `env.yaml`

Templates for your threat defense virtual version are available from the GitHub repository at FTDv OpenStack heat template.

Important Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

Procedure

Step 1 Deploy the infrastructure heat template file.

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

Example:

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

Step 2 Verify if the infrastructure stack is created successfully.

root@ucs-os-controller:$ openstack stack list

What to do next

Create the threat defense virtual instance on OpenStack.

Deploy the Threat Defense Virtual on OpenStack

Use the sample threat defense virtual heat template to deploy the threat defense virtual on OpenStack.

Before you begin

A heat template is required to deploy the threat defense virtual on OpenStack:

- `deploy_ftdv.yaml`

Templates for your threat defense virtual version are available from the GitHub repository at FTDv OpenStack heat template.

Important Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

Procedure

Step 1 Deploy the threat defense virtual heat template file (`deploy_ftdv.yaml`) to create the threat defense virtual instance.

root@ucs-os-controller:$ openstack stack create ftdv-stack -e env.yaml-t deploy_ftdv.yaml

Example:

```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+------------------------------+
| id                  | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name          | ftdv-stack                   |
| description         | FTDvtemplate                 |
| updated_time        | None                         |
| stack_status        | CREATE_IN_PROGRESS           |
| stack_status_reason | Stack CREATE started         |
+---------------------+------------------------------+
```

Step 2 Verify that your threat defense virtual stack is created successfully.

root@ucs-os-controller:$ openstack stack list

Example:

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack Status
    |
+--------------------------------------+-------------+----------------------------------+----------------+
```

```
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+-----------------+
```