Deploy the ASAv on OCI

You can deploy the ASAv on the Oracle Cloud Infrastructure (OCI).

Overview

OCI is a public cloud computing service that enables you to run your applications in a highly-available, hosted environment offered by Oracle.

The ASAv runs the same software as physical ASAvs to deliver proven security functionality in a virtual form factor. The ASAv can be deployed in the public OCI. It can then be configured to protect virtual and physical data center workloads that expand, contract, or shift their location over time.

OCI Compute Shapes

A shape is a template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance. The ASAv supports the following *Standard – General purpose* OCI shape types:

Table 1: Supported Compute Shapes for ASAv

OCI Shape	Supported ASAv Version	Attributes		Interfaces
		oCPUs	RAM (GB)	
Intel VM.Standard2.4	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21, and 9.22 and later	4	60	Minimum 4, Maximum 4
IntelVM.Standard2.8	9.15, 9.16, 9.17, 9.18, 9.19, 9.20, 9.21, and 9.22 and later	8	120	Minimum 4, Maximum 8

- The ASAv requires a minimum of 3 interfaces.
- In OCI, 1 oCPU is equal to 2 vCPUs.
- The maximum supported vCPUs is 16 (8 oCPUs).

You create an account on OCI, launch a compute instance using the Cisco ASA virtual firewall (ASAv) offering on the Oracle Cloud Marketplace, and choose an OCI shape.

Prerequisites

- Create an account on https://www.oracle.com/cloud/sign-in.html.
- License the ASAv. Until you license the ASAv, it will run in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Licenses: Smart Software Licensing .
- Interface requirements:
    - Management interface
    - Inside and outside interfaces
    - (Optional) Additional subnet (DMZ)
- Communications paths:
    - Management interface—Used to connect the ASAv to the ASDM; can't be used for through traffic.
    - Inside interface (required)—Used to connect the ASAv to inside hosts.
    - Outside interface (required)—Used to connect the ASAv to the public network.
    - DMZ interface (optional)—Used to connect the ASAv to the DMZ network.
- For ASAv system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations

Supported Features

The ASAv on OCI supports the following features:

- Deployment in the OCI Virtual Cloud Network (VCN)
- Maximum of 16 vCPUs (8 oCPUs) per instance
- Routed mode (default)
- Licensing – Only BYOL is supported
- Single Root I/O Virtualization (SR-IOV) is supported

Performance Tiers for ASAv Smart Licensing

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

Performance Tier	Instance Type (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv5	VM.Standard2.4 4 core/60 GB	100 Mbps	50
ASAv10	VM.Standard2.4 4 core/60 GB	1 Gbps	250
ASAv30	VM.Standard2.4 4 core/60 GB	2 Gbps	750
ASAv50	VM.Standard2.8 8 core/120 GB	NA	10,000
ASAv100	VM.Standard2.8 8 core/120 GB	NA	20,000

Unsupported Features

The ASAv on OCI does not support the following:

- ASAv native HA
- Transparent/inline/passive modes
- Multi-context mode
- IPv6

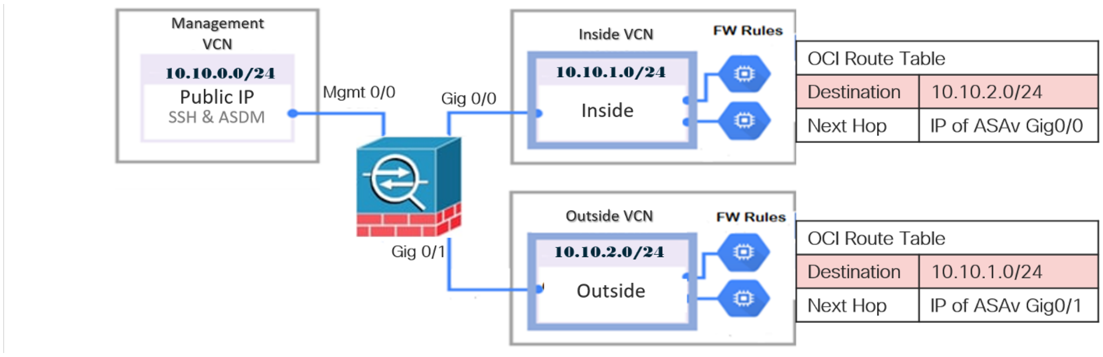
Limitations

- ASAv deployment on OCI does not support Mellanox 5 as vNICs in the SR-IOV mode.
- Separate routing rules required for ASAv for both static and DHCPconfiguration.

Sample Network Topology

The following figure shows the recommended network topology for the ASAv in Routed Firewall Mode with 3 subnets configured in OCI for the ASAv (management, inside, and outside).

Figure 1: Sample ASAv on OCI Deployment



OCI Route Table	
Destination	10.10.2.0/24
Next Hop	IP of ASAv Gig0/0

OCI Route Table	
Destination	10.10.1.0/24
Next Hop	IP of ASAv Gig0/1

Deploy the ASAv

The following procedures describe how to prepare your OCI environment and launch the ASAv instance. You log into the OCI portal, search the OCI Marketplace for the Cisco ASA virtual firewall (ASAv) offering, and launch the compute instance. After launching the ASAv, you must configure route tables to direct traffic to the firewall depending on the traffic's source and destination.

Create the Virtual Cloud Network (VCN)

You configure the Virtual Cloud Network (VCN) for your ASAv deployment. At a minimum, you need three VCNs, one for each interface of the ASAv.

You can continue with the following procedures to complete the Management VCN. Then you return to **Networking** to create VCNs for the inside and outside interfaces.

Before you begin

Note After you select a service from the navigation menu, the menu on the left includes the compartments list. Compartments help you organize resources to make it easier to control access to them. Your root compartment is created for you by Oracle when your tenancy is provisioned. An administrator can create more compartments in the root compartment and then add the access rules to control which users can see and take action in them. See the Oracle document "Managing Compartments" for more information.

Procedure

Step 1 Log into OCI and choose your region.

OCI is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 Choose **Networking** > **Virtual Cloud Networks** and click Create Virtual Cloud Networks.

Step 3 Enter a descriptive **Name** for your VCN, for example *ASAvManagement*.

Step 4 Enter a **CIDR block** for your VCN.

Step 5 Click **Create VCN**.

Create the Network Security Group

A network security group consists of a set of vNICs and a set of security rules that apply to those vNICs.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Network Security Groups**, and click **Create Network Security Group**.

Step 2 Enter a descriptive **Name** for your Network Security Group, for example *ASAv-Mgmt-Allow-22-443*.

Step 3 Click **Next**.

Step 4 Add your security rules:

a) Add a rule to allow TCP port 22 for SSH Access to ASAv console.

b) Add a rule to allow TCP port 443 for HTTPS Access to ASDM.

The ASAv can be managed via ASDM, which requires port 443 to be opened for HTTPS connections.

Step 5 Click **Create**.

Create the Internet Gateway

An Internet gateway is required to make your management subnet publicly accessible.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Internet Gateways**, and click **Create Internet Gateway**.

Step 2 Enter a descriptive **Name** for your Internet gateway, for example, *ASAv-IG*.

Step 3 Click **Create Internet Gateway**.

Step 4 Add the route to the Internet Gateway:

a) Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Route Tables**.

b) Click on the link for your default route table to add route rules.

c) Click **Add Route Rules**.

d) From the **Target Type** drop-down, select **Internet Gateway**.

e) Enter the Destination IPv4 CIDR Block, for example 0.0.0.0/0.

f) From the **Target Internet Gateway** drop-down, select the gateway you created.

g) Click **Add Route Rules**.

Create the Subnet

Each VCN will have one subnet, at a minimum. You'll create a Management subnet for the Management VCN. You'll also need an Inside subnet for the Inside VCN, and an Outside subnet for the Outside VCN.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Subnets**, and click **Create Subnet**.

Step 2 Enter a descriptive **Name** for your subnet, for example, *Management*.

Step 3 Select a **Subnet Type** (leave the recommended default of **Regional**).

Step 4 Enter a **CIDR Block**, for example 10.10.0.0/24. The internal (non-public) IP address for the subnet is taken from this CIDR block.

Step 5 Select one of the route tables you created previously from the **Route Table** drop-down.

Step 6 Select the **Subnet Access** for your subnet.

For the Management subnet, this must be **Public Subnet**.

Step 7 Select the **DHCP Option**.

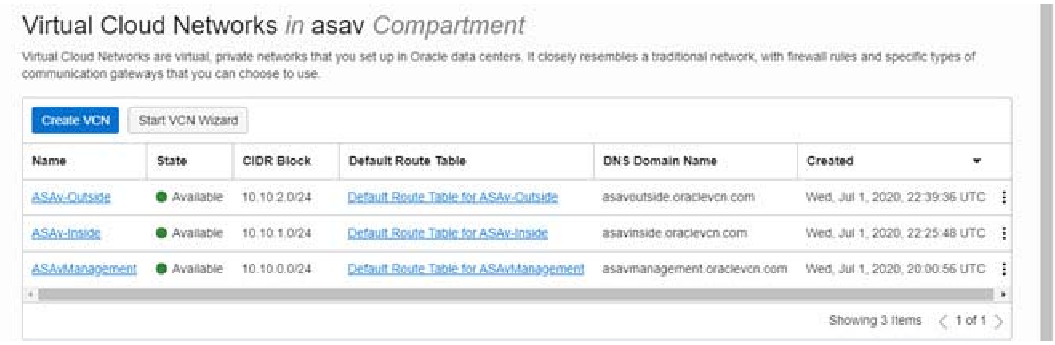
Step 8 Select a **Security List** that you created previously.

Step 9 Click **Create Subnet**.

What to do next

After you configure your VCNs (Management, Inside, Outside) you are ready to launch the ASAv. See the following figure for an example of the ASAv VCN configuration.

Figure 2: ASAv Cloud Networks



Virtual Cloud Networks *in* asav *Compartment*

Virtual Cloud Networks are virtual, private networks that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use.

Name	State	CIDR Block	Default Route Table	DNS Domain Name	Created
ASAv-Outside	● Available	10.10.2.0/24	Default Route Table for ASAv-Outside	asavoutside.oraclevcn.com	Wed, Jul 1, 2020, 22:39:36 UTC
ASAv-Inside	● Available	10.10.1.0/24	Default Route Table for ASAv-Inside	asavinside.oraclevcn.com	Wed, Jul 1, 2020, 22:25:48 UTC
ASAvManagement	● Available	10.10.0.0/24	Default Route Table for ASAvManagement	asavmanagement.oraclevcn.com	Wed, Jul 1, 2020, 20:00:56 UTC

Create the ASAv Instance on OCI

You deploy the ASAv on OCI via a Compute instance using the Cisco ASA virtual firewall (ASAv) offering on the Oracle Cloud Marketplace. You select the most appropriate machine shape based on characteristics such as the number of CPUs, amount of memory, and network resources.

Procedure

Step 1 Log into the OCI portal.

The region is displayed in the upper right corner of your screen. Make sure you are in the intended region.

Step 2 Choose **Marketplace** > **Applications**.

Step 3 Search Marketplace for “Cisco ASA virtual firewall (ASAv)” and choose the offering.

Step 4 Review the Terms and Conditions, and check the **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.**check box.

Step 5 Click **Launch Instance**.

Step 6 Enter a descriptive **Name** for your instance, for example, *ASAv-9-15*.

Step 7 Click **Change Shape** and select the shape with the number of oCPUs, the amount of RAM, and the number of interfaces required for the ASAv; for example, VM.Standard2.4 (see Table 1: Supported Compute Shapes for ASAv, on page 1).

Step 8 From the **Virtual Cloud Network** drop-down, choose the Management VCN.

Step 9 From the **Subnet** drop-down, choose the Management subnet if it's not autopopulated.

Step 10 Check **Use Network Security Groups to Control Traffic** and choose the security group you configured for the Management VCN.

Step 11 Click the **Assign a Public Ip Address** radio button.

Step 12 Under **Add SSH keys**, click the **Paste Public Keys** radio button and paste the SSH key.

Linux-based instances use an SSH key pair instead of a password to authenticate remote users. A key pair consists of a private key and public key. You keep the private key on your computer and provide the public key when you create an instance. See Managing Key Pairs on Linux Instances for guidelines.

Step 13 Click the **Show Advanced Options** link to expand the options.

Step 14 (Optional) Under **Initialization Script**, click the **Paste Cloud-Init Script** radio button to provide a day0 configuration for the ASAv. The day0 configuration is applied when the ASAv is launched.

The following example shows a sample day0 configuration you can copy and paste in the **Cloud-Init Script** field:

See the ASA Configuration Guides and the ASA Command Reference for complete information on the ASA commands.

Important
When you copy text from this example, you should validate the script in a third-party text editor or validation engine to prevent format errors and remove invalid Unicode characters.

```
!ASA Version 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute

no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
```

```
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
aaa authentication ssh console LOCAL
```

Step 15 Click **Create**.

What to do next

Monitor the ASAv instance, which shows the state as Provisioning after you click the **Create** button.

Important It's important to monitor the status. As soon as the ASAv instance goes from Provisioning to Running state you need to attach the VNICs as required before the ASAv boot completes.

Attach the Interfaces

The ASAv enters the Running state with one VNIC attached (see **Compute** > **Instances** > **Instance Details** > **Attached VNICs**). This is referred to as the Primary VNIC, and maps to the Management VCN. Before the ASAv completes the first boot, you need to attach the VNICs for the other VCN subnets you created previously (inside, outside) so that the VNICs are correctly detected on ASAv.

Procedure

Step 1 Select your newly launched ASAv instance.

Step 2 Choose **Attached VNICs** > **Create VNIC**.

Step 3 Enter a descriptive **Name** for your VNIC, for example *Inside*.

Step 4 Select the VCN from the **Virtual Cloud Network** drop-down.

Step 5 Select your subnet from the **Subnet** drop-down.

Step 6 Check **Use Network Security Groups to Control Traffic** and choose the security group you configured for the selected VCN.

Step 7 Check **Skip Source Destination Check** Network Security Groups to Control Traffic.

Step 8 (Optional) Specify a **Private IP Address**. This is only required if you want to choose a particular IP for the VNIC.

If you do not specify an IP, OCI will assign an IP address from the CIDR block you assigned to the subnet.

Step 9 Click **Save Changes** to create the VNIC.

Step 10 Repeat this procedure for each VNIC your deployment requires.

Add Route Rules for the Attached VNICs

Add route table rules to the inside and outside route tables.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > and click the default route table associated with the VCN (inside or outside).

Step 2 Click **Add Route Rules**.

Step 3 From the **Target Type** drop-down, select **Private IP**.

Step 4 From the **Destination Type** drop-down, select **CIDR Block**.

Step 5 Enter the **Destination IPv4 CIDR Block**, for example, 0.0.0.0/0.

Step 6 Enter the private IP address of the VNIC in the **Target Selection** field.

If you did not explicitly assign an IP address to the VNIC, you can find the auto-assigned IP address from the VNIC details (**Compute** > **Instances** > **Instance Details** > **Attached VNICs**).

Step 7 Click **Add Route Rules**.

Step 8 Repeat this procedure for each VNIC your deployment requires.

Note
Separate routing rules required for ASA Virtual (Static and DHCP) configuration.

Access the ASAv Instance on OCI

You can connect to a running instance by using a Secure Shell (SSH) connection.

- Most UNIX-style systems include an SSH client by default.
- Windows 10 and Windows Server 2019 systems should include the OpenSSH client, which you'll need if you created your instance using the SSH keys generated by Oracle Cloud Infrastructure.
- For other Windows versions you can download PuTTY, the free SSH client from http://www.putty.org.

Prerequisites

You'll need the following information to connect to the instance:

- The public IP address of the instance. You can get the address from the Instance Details page in the Console. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. Then, select your instance. Alternatively, you can use the Core Services API ListVnicAttachments and GetVnic operations.
- The username and password of your instance.
- The full path to the private key portion of the SSH key pair that you used when you launched the instance. For more information about key pairs, see Managing Key Pairs on Linux Instances.

Note You can log in to the ASAv instance using the credentials specified in the day0 configuration, or by using the SSH key pair you created during the instance launch.

Connect to the ASAv Instance Using SSH

To connect to the ASAv instance from a Unix-style system, log in to the instance using SSH.

Procedure

Step 1 Use the following command to set the file permissions so that only you can read the file:

```
$ chmod 400 <private_key>
```

Where:

`<private_key>` is the full path and name of the file that contains the private key associated with the instance you want to access.

Step 2 Use the following SSH command to access the instance.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Where:

`<private_key>` is the full path and name of the file that contains the private key associated with the instance you want to access.

`<username>` is the username for the ASAv instance.

`<public-ip-address>` is your instance IP address that you retrieved from the Console.

Connect to the ASAv Instance Using OpenSSH

To connect to the ASAv instance from a Windows system, log in to the instance using OpenSSH.

Procedure

Step 1 If this is the first time you are using this key pair, you must set the file permissions so that only you can read the file.

Do the following:

a) In Windows Explorer, navigate to the private key file, right-click the file, and then click **Properties**.
b) On the **Security** tab, click **Advanced**.
c) Ensure that the **Owner** is your user account.
d) Click **Disable Inheritance**, and then select **Convert inherited permissions into explicit permissions on this object**.
e) Select each permission entry that is not your user account and click **Remove**.

f) Ensure that the access permission for your user account is **Full control**.

g) Save your changes.

Step 2 To connect to the instance, open Windows PowerShell and run the following command:

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Where:

`<private_key>` is the full path and name of the file that contains the private key associated with the instance you want to access.

`<username>` is the username for the ASAv instance.

`<public-ip-address>` is your instance IP address that you retrieved from the Console.

Connect to the ASAv Instance Using PuTTY

To connect to the ASAv instance from a Windows system using PuTTY:

Procedure

Step 1 Open PuTTY.

Step 2 In the **Category** pane, select **Session** and enter the following:

- **Host Name (or IP address):**

  ```
  <username>@<public-ip-address>
  ```

  Where:

  `<username>` is the username for the ASAv instance.

  `<public-ip-address>` is your instance public IP address that you retrieved from the Console.

- **Port:** 22
- **Connection type:** SSH

Step 3 In the **Category** pane, expand **Window**, and then select **Translation**.

Step 4 In the **Remote character set** drop-down list, select **UTF-8**.

The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.

Step 5 In the **Category** pane, expand **Connection**, expand **SSH**, and then click **Auth**.

Step 6 Click **Browse**, and then select your private key.

Step 7 Click **Open** to start the session.

If this is your first time connecting to the instance, you might see a message that the server's host key is not cached in the registry. Click **Yes** to continue the connection.