# Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide

Version 9.4

**Published:** May 12, 2015
**Revised:** August 31, 2015

# Introduction to the Cisco ASAv

The Cisco Adaptive Security Virtual Appliance (ASAv) brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments.

You can manage and monitor the ASAv using ASDM or CLI. Other management options may be available.



## Prerequisites for the ASAv

For hypervisor support, see Cisco ASA Compatibility.

## Guidelines for the ASAv

### Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

### Failover Guidelines

For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

### Unsupported ASA Features

The ASAv does not support the following ASA features:

- Clustering
- Multiple context mode
- Active/Active failover
- EtherChannels
- Shared AnyConnect Premium Licenses

## Licensing for the ASAv

The ASAv uses Cisco Smart Software Licensing. For detailed information, see Smart Software Licensing for the ASAv.

| Model | License Requirement |
|---|---|
| ASAv5 | Standard license<br>See the following specifications:<br>■ 100 Mbps Throughput<br>■ 1 vCPU<br>■ 2 GB RAM<br>■ 100,000 concurrent firewall connections<br>■ Does not support AWS |
| ASAv10 | Standard license<br>See the following specifications:<br>■ 1 Gbps Throughput<br>■ 1 vCPU<br>■ 2 GB RAM<br>■ 100,000 concurrent firewall connections<br>■ Supports AWS |
| ASAv30 | Standard license<br>See the following specifications:<br>■ 2 Gbps Throughput<br>■ 4 vCPUs<br>■ 8 GB RAM<br>■ 500,000 concurrent firewall connections<br>■ Supports AWS |

**Note:** You must install a smart license on the ASAv. Until you install a license, throughput is limited to 100 Kbps so you can perform preliminary connectivity tests. A smart license is required for regular operation.

# ASAv Interfaces and Virtual NICs

As a guest on a virtualized platform, the ASAv utilizes the network interfaces of the underlying physical platform. Each ASAv interface maps to a virtual NIC (vNIC).



## ASAv Interfaces

The ASAv includes the following Gigabit Ethernet interfaces:

- Management 0/0
- GigabitEthernet 0/0 through 0/8. Note that the GigabitEthernet 0/8 is used for the failover link when you deploy the ASAv as part of a failover pair.

## Supported vNICs

The ASAv supports the following vNICs:

| vNIC Type | Hypervisor Support | | ASAv Version | Notes |
|---|---|---|---|---|
| | VMware | KVM | | |
| e1000 | **Yes** | **Yes** | 9.2(1) and later | VMware default. |
| Virtio | No | **Yes** | 9.3(2.200) and later | KVM default. |

# Deploy the ASAv Using VMware

You can deploy the ASAv using VMware.



## VMware Feature Support for the ASAv

The following table lists the VMware feature support for the ASAv.

**Table 1 VMware Feature Support for the ASAv**

| Feature | Description | Support (Yes/No) | Comment |
|---|---|---|---|
| Cold clone | The VM is powered off during cloning. | Yes | – |
| DRS | Used for dynamic resource scheduling and distributed power management. | Yes | See VMware guidelines. |
| Hot add | The VM is running during an addition. | No | – |
| Hot clone | The VM is running during cloning. | No | – |
| Hot removal | The VM is running during removal. | No | – |
| Snapshot | The VM freezes for a few seconds. | Yes | Use with care. You may lose traffic. Failover may occur. |
| Suspend and resume | The VM is suspended, then resumed. | Yes | – |
| vCloud Director | Allows automated deployment of VMs. | No | – |
| VM migration | The VM is powered off during migration. | Yes | – |
| vMotion | Used for live migration of VMs. | Yes | – |
| VMware FT | Used for HA on VMs. | No | Use ASAv failover for ASAv VM failures. |
| VMware HA | Used for ESX and server failures. | Yes | Use ASAv failover for ASAv VM failures. |

**Table 1 VMware Feature Support for the ASAv (continued)**

| Feature | Description | Support (Yes/No) | Comment |
|---|---|---|---|
| VMware HA with VM heartbeats | Used for VM failures. | No | Use ASAv failover for ASAv VM failures. |
| VMware vSphere Standalone Windows Client | Used to deploy VMs. | Yes | – |
| VMware vSphere Web Client | Used to deploy VMs. | Yes | – |

# Prerequisites for the ASAv and VMware

You can deploy the ASAv using the VMware vSphere Web Client, vSphere standalone client, or the OVF tool. See Cisco ASA Compatibility for system requirements.

### Security Policy for a vSphere Standard Switch

For a vSphere switch, you can edit Layer 2 security policies and apply security policy exceptions for port groups used by the ASAv interfaces. See the following default settings:

- Promiscuous Mode: **Reject**
- MAC Address Changes: **Accept**
- Forged Transmits: **Accept**

You may need to modify these settings for the following ASAv configurations. See the vSphere documentation for more information.

**Table 2 Port Group Security Policy Exceptions**

| Security Exception | Routed Firewall Mode | | Transparent Firewall Mode | |
|---|---|---|---|---|
| | No Failover | Failover | No Failover | Failover |
| Promiscuous Mode | <Any> | <Any> | Accept | Accept |
| MAC Address Changes | <Any> | Accept | <Any> | Accept |
| Forged Transmits | <Any> | Accept | Accept | Accept |

# Guidelines for the ASAv and VMware

### OVF File Guidelines

The selection of the asav-vi.ovf or asav-esxi.ovf file is based on the deployment target:

- asav-vi–For deployment on vCenter
- asav-esxi–For deployment on ESXi (no vCenter)

### Failover Guidelines

For failover deployments, make sure that the standby unit has the same model license; for example, both units should be ASAv30s.

### IPv6 Guidelines

You cannot specify IPv6 addresses for the management interface when you first deploy the ASAv OVF file using the VMware vSphere Web Client; you can later add IPv6 addressing using ASDM or the CLI.

### Additional Guidelines and Limitations

- The ASAv OVF deployment does not support localization (installing the components in non-English mode). Be sure that the VMware vCenter and the LDAP servers in your environment are installed in an ASCII-compatible mode.
- You must set your keyboard to United States English before installing the ASAv and for using the VM console.
- The memory allocated to the ASAv is sized specifically for the Throughput Level. Do not change the memory setting or any vCPU hardware settings in the **Edit Settings** dialog box unless you are requesting a license for a different Throughput Level. Under-provisioning can affect performance, and over-provisioning causes the ASAv to warn you that it will reload; after a waiting period (24 hours for 100-125% over-provisioning; 1 hour for 125% and up), the ASAv will reload.

  **Note:** If you need to change the memory or vCPU hardware settings, use only the values documented in Licensing for the ASAv, page 3. Do not use the VMware-recommended memory configuration minimum, default, and maximum values.

  Use the ASAv **show vm** and **show cpu** commands or the ASDM **Home > Device Dashboard > Device Information > Virtual Resources** tab or the **Monitoring > Properties > System Resources Graphs > CPU** pane to view the resource allocation and any resources that are over- or under-provisioned.
- During ASAv deployment, if you have a host cluster, you can either provision storage locally (on a specific host) or on a shared host. However, if you try to vMotion the ASAv to another host, using any kind of storage (SAN or local) causes an interruption in connectivity.
- If you are running ESXi 5.0, the vSphere Web Client is not supported for ASAv OVF deployment; use the vSphere client instead.

# Unpack the ASAv Software and Create a Day 0 Configuration File for VMware

You can prepare a Day 0 configuration file before you launch the ASAv. This file is a text file that contains the ASAv configuration that will be applied when the ASAv is launched. This initial configuration is placed into a text file named “day0-config” in a working directory you chose, and is manipulated into a day0.iso file that is mounted and read on first boot. At the minimum, the Day 0 configuration file must contain commands that will activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration. A default day0.iso containing an empty day0-config is provided with the release. The day0.iso file (either your custom day0.iso or the default day0.iso) must be available during first boot.

**Note:** To automatically license the ASAv during initial deployment, place the Smart Licensing Identity (ID) Token that you downloaded from the Cisco Smart Software Manager in a text file named ‘idtoken’ in the same directory as the Day 0 configuration file.

**Note:** If you want to deploy the ASAv in transparent mode, you must use a known running ASA config file in transparent mode as the Day 0 configuration file. This does not apply to a Day 0 configuration file for a routed firewall.

**Note:** We are using Linux in this example, but there are similar utilities for Windows.

### Procedure

1. Download the ZIP file from Cisco.com, and save it to your local disk:

   http://www.cisco.com/go/asa-software

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

2. Unzip the file into a working directory. Do not remove any files from the directory. The following files are included:
   - asav-vi.ovf—For vCenter deployments.
   - asav-esxi.ovf—For non-vCenter deployments.
   - boot.vmdk—Boot disk image.
   - disk0.vmdk—ASAv disk image.
   - day0.iso—An ISO containing a day0-config file and optionally an idtoken file.
   - asav-vi.mf—Manifest file for vCenter deployments.
   - asav-esxi.mf—Manifest file for non-vCenter deployments.
3. Enter the CLI configuration for the ASAv in a text file called “day0-config”. Add interface configurations for the three interfaces and any other configuration you want.

   The fist line should begin with the ASA version. The day0-config should be a valid ASA configuration. The best way to generate the day0-config is to copy the desired parts of a running config from an existing ASA or ASAv. The order of the lines in the day0-config is important and should match the order seen in an existing show run command output.

   Example:

```
ASA Version 9.4.1
!
interface management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
interface gigabitethernet0/0
nameif inside
security-level 100
ip address 10.1.1.2 255.255.255.0
no shutdown
interface gigabitethernet0/1
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
no shutdown
http server enable
http 192.168.1.0 255.255.255.0 management
crypto key generate rsa modulus 1024
username AdminUser password paSSw0rd
ssh 192.168.1.0 255.255.255.0 management
aaa authentication ssh console LOCAL
call-home
http-proxy 10.1.1.1 port 443
license smart
feature tier standard
throughput level 2G
```

4. (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your PC.
5. (Optional) Copy the ID token from the download file and put it in a text file named ‘idtoken’ that only contains the ID token.

   The Identity Token automatically registers the ASAv with the Smart Licensing server.
6. Generate the virtual CD-ROM by converting the text file to an ISO file:

```
stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
```

```
I: input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size (bytes): 10
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

7. Compute a new SHA1 value on Linux for the day0.iso:

```
openssl dgst -sha1 day0.iso
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66 day0.iso
```

8. Include the new checksum in the asav-vi.mf file in the working directory and replace the day0.iso SHA1 value with the newly generated one.

   Example.mf file

```
SHA1(asav-vi.ovf)= de0f1878b8f1260e379ef853db4e790c8e92f2b2
SHA1(disk0.vmdk)= 898b26891cc68fa0c94ebd91532fc450da418b02
SHA1(boot.vmdk)= 6b0000ddebfc38ccc99ac2d4d5dbfb8abfb3d9c4
SHA1(day0.iso)= e5bee36e1eb1a2b109311c59e2f1ec9f731ecb66
```

9. Copy the day0.iso file into the directory where you unzipped the ZIP file. You will overwrite the default (empty) day0.iso file.

   When any VM is deployed from this directory, the configuration inside the newly generated day0.iso is applied.

# Deploy the ASAv Using the VMware vSphere Web Client

This section describes how to deploy the ASAv using the VMware vSphere Web Client. The Web Client requires vCenter. If you do not have vCenter, see Deploy the ASAv Using the VMware vSphere Standalone Client and a Day 0 Configuration, page 15 or Deploy the ASAv Using the OVF Tool and Day 0 Configuration, page 16.



## Access the vSphere Web Client and Install the Client Integration Plug-In

This section describes how to access the vSphere Web Client. This section also describes how to install the Client Integration Plug-In, which is required for ASAv console access. Some Web Client features (including the plug-in) are not supported on the Macintosh. See the VMware website for complete client support information.

### Procedure

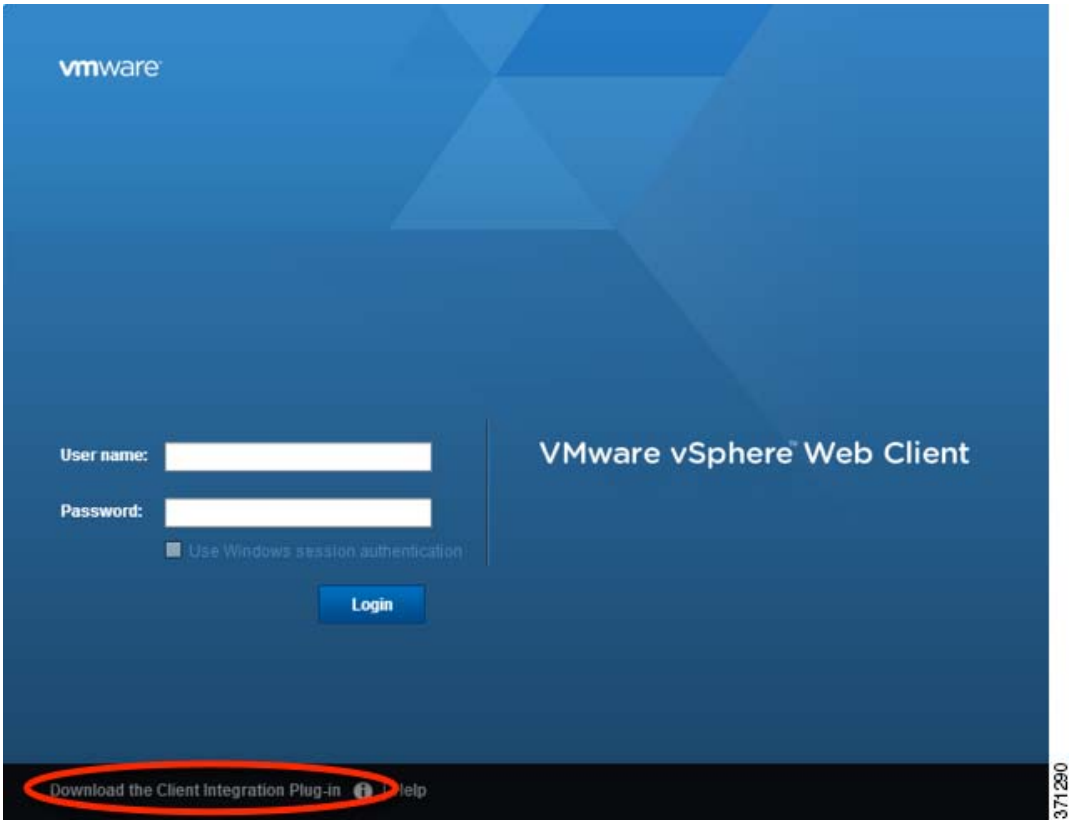
1. Launch the VMware vSphere Web Client from your browser:

   **https://***vCenter_server*:*port*/**vsphere-client/**

   By default, the port is 9443.

2. (One time only) Install the Client Integration Plug-in so that you can access the ASAv console.

   a. In the login screen, download the plug-in by clicking **Download the Client Integration Plug-in**.




b. Close your browser and then install the plug-in using the installer.

c. After the plug-in installs, reconnect to the vSphere Web Client.

3. Enter your username and password, and click **Login**, or check the **Use Windows session authentication** check box (Windows only).

# Deploy the ASAv Using the VMware vSphere Web Client

To deploy the ASAv, use the VMware vSphere Web Client (or the vSphere Client) and a template file in the open virtualization format (OVF). You use the Deploy OVF Template wizard in the vSphere Web Client to deploy the Cisco package for the ASAv. The wizard parses the ASAv OVF file, creates the virtual machine on which you will run the ASAv, and installs the package.

Most of the wizard steps are standard for VMware. For additional information about the Deploy OVF Template, see the VMware vSphere Web Client online help.

### Before You Begin

You must have at least one network configured in vSphere (for management) before you deploy the ASAv.

### Procedure

1. Download the ASAv ZIP file from Cisco.com, and save it to your PC:

   http://www.cisco.com/go/asa-software

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

2. In the vSphere Web Client **Navigator** pane, click **vCenter**.

3. Click **Hosts and Clusters**.

4. Right-click the data center, cluster, or host where you want to deploy the ASAv, and choose **Deploy OVF Template**.

   The **Deploy OVF Template** wizard appears.

5. Follow the wizard screens as directed.

6. In the **Setup networks** screen, map a network to each ASAv interface that you want to use.

   The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the Edit Settings dialog box. After you deploy, right-click the ASAv instance, and choose **Edit Settings** to access the **Edit Settings** dialog box. However that screen does not show the ASAv interface IDs (only Network Adapter IDs). See the following concordance of Network Adapter IDs and ASAv interface IDs:

| Network Adapter ID | ASAv Interface ID |
|---|---|
| Network Adapter 1 | Management0/0 |
| Network Adapter 2 | GigabitEthernet0/0 |
| Network Adapter 3 | GigabitEthernet0/1 |
| Network Adapter 4 | GigabitEthernet0/2 |
| Network Adapter 5 | GigabitEthernet0/3 |
| Network Adapter 6 | GigabitEthernet0/4 |
| Network Adapter 7 | GigabitEthernet0/5 |
| Network Adapter 8 | GigabitEthernet0/6 |
| Network Adapter 9 | GigabitEthernet0/7 |
| Network Adapter 10 | GigabitEthernet0/8 |

   You do not need to use all ASAv interfaces; however, the vSphere Web Client requires you to assign a network to all interfaces. For interfaces you do not intend to use, you can simply leave the interface disabled within the ASAv configuration. After you deploy the ASAv, you can optionally return to the vSphere Web Client to delete the extra interfaces from the Edit Settings dialog box. For more information, see the vSphere Web Client online help.

   **Note:** For failover/HA deployments, GigabitEthernet 0/8 is pre-configured as the failover interface.

7. If your network uses an HTTP proxy for Internet access, you must configure the proxy address for smart licensing in the **Smart Call Home Settings** area. This proxy is also used for Smart Call Home in general.

8. For failover/HA deployments, in the **Customize template** screen:

   - Specify the standby management IP address.

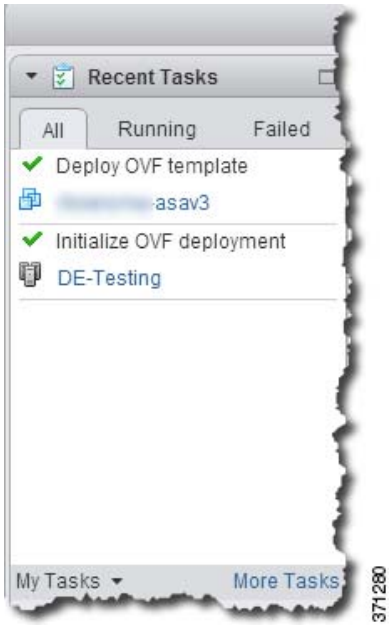
     When you configure your interfaces, you must specify an active IP address and a standby IP address on the same network. When the primary unit fails over, the secondary unit assumes the IP addresses and MAC addresses of the primary unit and begins passing traffic. The unit that is now in a standby state takes over the standby IP addresses and MAC addresses. Because network devices see no change in the MAC to IP address pairing, no ARP entries change or time out anywhere on the network.

   - Configure the failover link settings in the **HA Connection Settings** area.

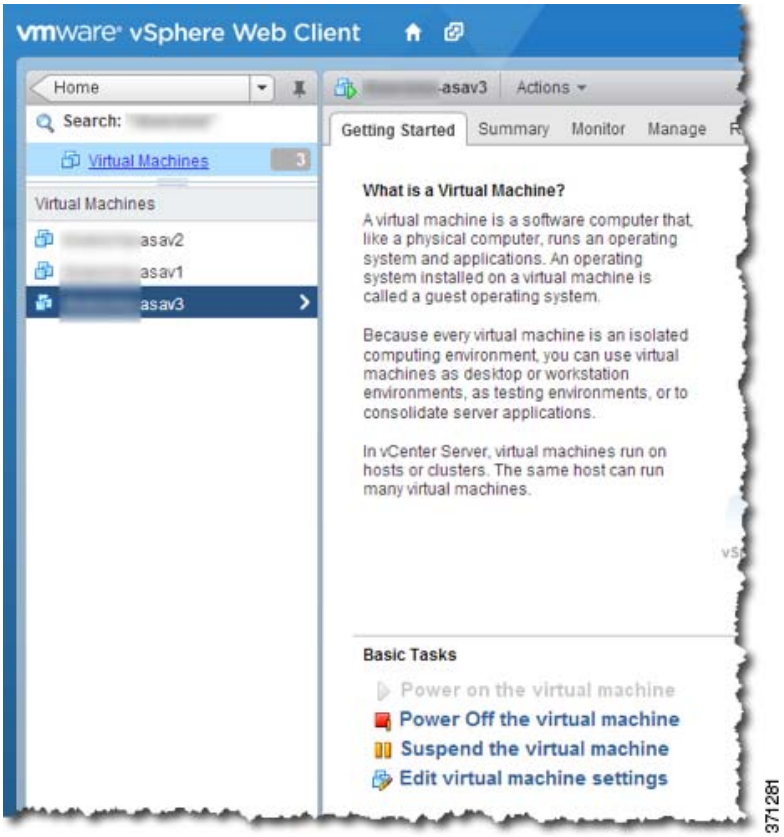
     The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit. GigabitEthernet 0/8 is pre-configured as the failover link. Enter the active and standby IP addresses for the link on the same network.

9. After you complete the wizard, the vSphere Web Client processes the VM; you can see the “Initialize OVF deployment” status in the **Global Information** area **Recent Tasks** pane.


When it is finished, you see the Deploy OVF Template completion status.




The ASAv VM instance then appears under the specified data center in the Inventory.




10. If the ASAv VM is not yet running, click **Power On the virtual machine**.

    Wait for the ASAv to boot up before you try to connect with ASDM or to the console. When the ASAv starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASAv system configuration. It then automatically restarts the boot process until it is up and running. This double boot process only occurs when you first deploy the ASAv. To view bootup messages, access the ASAv console by clicking the **Console** tab.

11. For failover/HA deployments, repeat this procedure to add the secondary unit. See the following guidelines:

    - Set the same throughput level as the primary unit.
    - Enter the *exact same IP address settings* as for the primary unit. The bootstrap configurations on both units are identical except for the parameter identifying a unit as primary or secondary.

**Note:** To successfully register the ASAv with the Cisco Licensing Authority, the ASAv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

# Deploy the ASAv Using the VMware vSphere Standalone Client and a Day 0 Configuration

To deploy the ASAv, use the VMware vSphere Client and the open virtualization format (OVF) template file (asav-vi.ovf for a vCenter deployment or asav-esxi.ovf for a non-vCenter deployment). You use the Deploy OVF Template wizard in the vSphere Client to deploy the Cisco package for the ASAv. The wizard parses the ASAv OVF file, creates the virtual machine on which you will run the ASAv, and installs the package.

Most of the wizard steps are standard for VMware. For additional information about the Deploy OVF Template wizard, see the VMware vSphere Client online help.

### Before You Begin

- You must have at least one network configured in vSphere (for management) before you deploy the ASAv.
- Follow the steps in Unpack the ASAv Software and Create a Day 0 Configuration File for VMware, page 9 to create the Day 0 configuration.

### Procedure

1. Launch the VMware vSphere Client and choose **File > Deploy OVF Template**.

   The Deploy OVF Template wizard appears.
2. Browse to the working directory where you unzipped the asav-vi.ovf file and select it.
3. The OVF Template details are shown. Proceed through the following screens. You do not have to change any configuration if you choose to use a custom Day 0 configuration file.
4. A summary of the deployment settings is shown in the last screen. Click **Finish** to deploy the VM.
5. Power on the ASAv, open the VMware console, and wait for the second boot.
6. SSH to the ASAv and complete your desired configuration. If you didn¡¦t have all the configuration that you wanted in the Day 0 configuration file, open a VMware console and complete the necessary configuration.

   The ASAv is now fully operational.

# Deploy the ASAv Using the OVF Tool and Day 0 Configuration

### Before You Begin

- The day0.iso file is required when you are deploying the ASAv using the OVF tool. You can use the default empty day0.iso file provided in the ZIP file, or you can use a customized Day 0 configuration file that you generate. See Unpack the ASAv Software and Create a Day 0 Configuration File for VMware, page 9 for creating a Day 0 configuration file.
- Make sure the OVF tool is installed on a Linux or Windows PC and that it has connectivity to your target ESXi server.

### Procedure

1. Verify the OVF tool is installed:

   ```
   linuxprompt# which ovftool
   ```
2. Create a .cmd file with the desired deployment options:

   Example:

   ```
   linuxprompt# cat launch.cmd
   ovftool \
   --name="asav-941-demo" \
   --powerOn \
   --deploymentOption=ASAv30 \
   --diskMode=thin \
   --datastore=datastore1 \
   --acceptAllEulas \
   --net:Management0-0="Portgroup_Mgmt" \
   --net:GigabitEthernet0-1="Portgroup_Inside" \
   --net:GigabitEthernet0-0="Portgroup_Outside" \
   --prop:HARole=Standalone \
   asav-esxi.ovf \
   vi://root@10.1.2.3/
   ```
3. Execute the cmd file:

```
linuxprompt# ./launch.cmd
```

The ASAv is powered on; wait for the second boot.

4. SSH to the ASAv to complete configuration as desired. If more configuration is required, open the VMware console to the ASAv and apply the necessary configuration.

   The ASAv is now fully operational.

# Access the ASAv Console

In some cases with ASDM, you may need to use the CLI for troubleshooting. By default, you can access the built-in VMware vSphere console. Alternatively, you can configure a network serial console, which has better capabilities, including copy and paste.

- Use the VMware vSphere Console, page 17
- Configure a Network Serial Console Port, page 18

## Use the VMware vSphere Console

For initial configuration or troubleshooting, access the CLI from the virtual console provided through the VMware vSphere Web Client. You can later configure CLI remote access for Telnet or SSH.

### Before You Begin

For the vSphere Web Client, install the Client Integration Plug-In, which is required for ASAv console access.

### Procedure

1. In the VMware vSphere Web Client, right-click the ASAv instance in the Inventory, and choose **Open Console**. Or you can click **Launch Console** on the **Summary** tab.
2. Click in the console and press **Enter**. Note: Press **Ctrl + Alt** to release the cursor.

   If the ASAv is still starting up, you see bootup messages.

   When the ASAv starts up for the first time, it reads parameters provided through the OVF file and adds them to the ASAv system configuration. It then automatically restarts the boot process until it is up and running. This double boot process only occurs when you first deploy the ASAv.

   **Note:** Until you install a license, throughput is limited to 100 Kbps so that you can perform preliminary connectivity tests. A license is required for regular operation. You also see the following messages repeated on the console until you install a license:

   ```
   Warning: ASAv platform license state is Unlicensed.
   Install ASAv platform license for full functionality.
   ```

   You see the following prompt:

   ```
   ciscoasa>
   ```

   This prompt indicates that you are in user EXEC mode. Only basic commands are available from user EXEC mode.
3. Access privileged EXEC mode:

   ```
   ciscoasa> enable
   ```

   The following prompt appears:

   ```
   Password:
   ```

4. Press the **Enter** key to continue. By default, the password is blank. If you previously set an enable password, enter it instead of pressing Enter.

   The prompt changes to:

   ```
   ciscoasa#
   ```

   All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

   To exit privileged mode, enter the **disable**, **exit**, or **quit** command.

5. Access global configuration mode:

   ```
   ciscoasa# configure terminal
   ```

   The prompt changes to the following:

   ```
   ciscoasa(config)#
   ```

   You can begin to configure the ASAv from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

## Configure a Network Serial Console Port

For a better console experience, you can configure a network serial port singly or attached to a virtual serial port concentrator (vSPC) for console access. See the VMware vSphere documentation for details about each method. On the ASAv, you must send the console output to a serial port instead of to the virtual console. This section describes how to enable the serial port console.

### Procedure

1. Configure a network serial port in VMware vSphere. See the VMware vSphere documentation.
2. On the ASAv, create a file called “use_ttyS0” in the root directory of disk0. This file does not need to have any contents; it just needs to exist at this location:

   disk0:/use_ttyS0

   - From ASDM, you can upload an empty text file by that name using the **Tools > File Management** dialog box.
   - At the vSphere console, you can copy an existing file (any file) in the file system to the new name. For example:

     ```
     ciscoasa(config)# cd coredumpinfo
     ciscoasa(config)# copy coredump.cfg disk0:/use_ttyS0
     ```

3. Reload the ASAv.

   - From ASDM, choose **Tools > System Reload**.
   - At the vSphere console, enter **reload**.

   The ASAv stops sending to the vSphere console, and instead sends to the serial console.

4. Telnet to the vSphere host IP address and the port number you specified when you added the serial port; or Telnet to the vSPC IP address and port.

# Upgrade the vCPU or Throughput License

The ASAv uses a throughput license, which affects the number of vCPUs you can use.

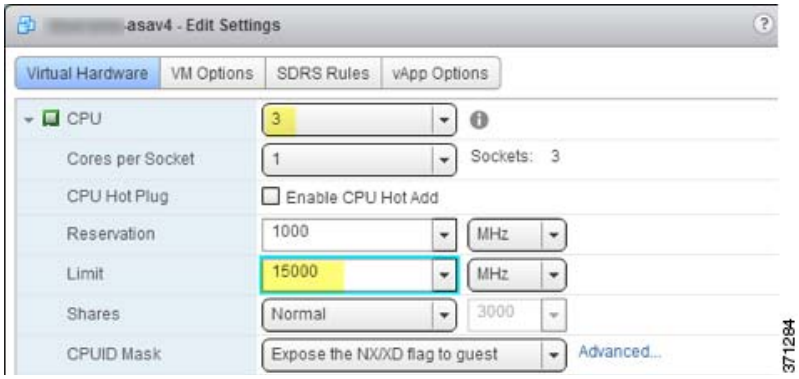
If you want to increase (or decrease) the number of vCPUs for your ASAv, you can request a new license, apply the new license, and change the VM properties in VMware to match the new values.

**Note:** The assigned vCPUs must match the ASAv Virtual CPU license or Throughput license. The RAM must also be sized correctly for the vCPUs. When upgrading or downgrading, be sure to follow this procedure and reconcile the license and vCPUs immediately. The ASAv does not operate properly when there is a persistent mismatch.

### Procedure

1. Request a new license.
2. Apply the new license. For failover pairs, apply new licenses to both units.
3. Do one of the following, depending on if you use failover or not:
   - Failover—In the vSphere Web Client, power off the *standby* ASAv. For example, click the ASAv and then click **Power Off the virtual machine**, or right-click the ASAv and choose **Shut Down Guest OS**.
   - No Failover—In the vSphere Web Client, power off the ASAv. For example, click the ASAv and then click **Power Off the virtual machine**, or right-click the ASAv and choose **Shut Down Guest OS**.
4. Click the ASAv and then click **Edit Virtual machine settings** (or right-click the ASAv and choose **Edit Settings**).

   The **Edit Settings** dialog box appears.
5. Refer to the CPU memory requirement in Licensing for the ASAv, page 3 to determine the correct values for the new vCPU license.
6. On the **Virtual Hardware** tab, for the **CPU**, choose the new value from the drop-down list.




7. For the **Memory**, enter the new value for the RAM.
8. Click **OK**.
9. Power on the ASAv. For example, click **Power On the Virtual Machine**.
10. For failover pairs:
    a. Open a console to the active unit or Launch ASDM on the active unit.
    b. After the standby unit finishes starting up, failover to the standby unit
       - ASDM: Choose **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.
       - CLI: ciscoasa# **failover active**
    c. Repeat Steps 3 through 9 for the active unit.

### Related Topics

- Licensing for the ASAv, page 3

# Deploy the ASAv Using KVM

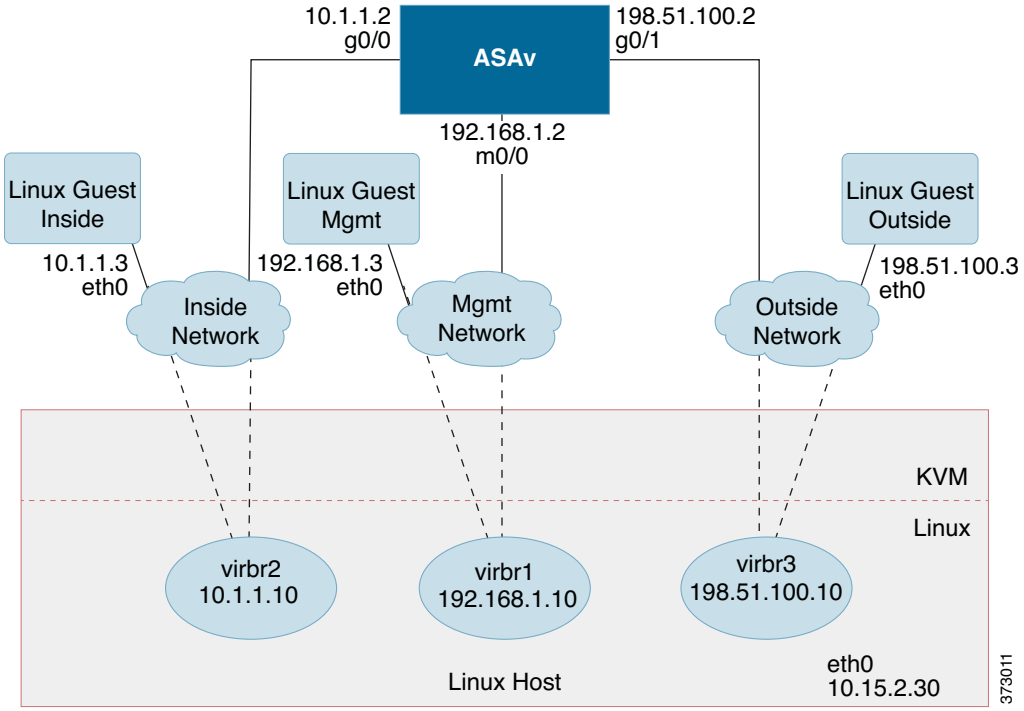
You can deploy the ASAv using the Kernel-based Virtual Machine (KVM).



## About ASAv Deployment Using KVM

Figure 1 on page -15 shows a sample network topology with ASAv and KVM. The procedures described in this chapter are based on the sample topology. You requirements will dictate the exact procedures you need. The ASAv acts as the firewall between the inside and outside networks. A separate management network is also configured.

**Figure 1 Sample ASAv Deployment Using KVM**



# Prerequisites for the ASAv and KVM

- Download the ASAv qcow2 file from Cisco.com and put it on your Linux host:

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

- For the purpose of the sample deployment in this document, we are assuming you are using Ubuntu 14.04 LTS. Install the following packages on top of the Ubuntu 14.04 LTS host:
  - qemu-kvm
  - libvirt-bin
  - bridge-utils
  - virt-manager
  - virtinst
  - virsh tools
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput of the ASAv on KVM by tuning your host. For generic host-tuning concepts, see Network Function Virtualization Packet Processing Performance of Virtualized Platforms with Linux and Intel Architecture.
- Useful optimizations for Ubuntu 14.04 include the following:
  - macvtap—High performance Linux bridge; you can use macvtap instead of a Linux bridge. Note that you must configure specific settings to use macvtap instead of the Linux bridge.
  - Transparent Huge Pages—Increases memory page size and is on by default in Ubuntu 14.04.
  - Hyperthread disabled—Reduces two vCPUs to one single core.
  - txqueuelength—Increases the default txqueuelength to 4000 packets and reduces drop rate.
  - pinning—Pins qemu and vhost processes to specific CPU cores; under certain conditions, pinning is a significant boost to performance.
- For information on optimizing a RHEL-based distribution, see Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide.
- For KVM system requirements, see Cisco ASA Compatibility.

# Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the ASAv. This file is a text file that contains the ASAv configuration that will be applied when the ASAv is launched. This initial configuration is placed into a text file named “day0-config” in a working directory you chose, and is manipulated into a day0.iso file that is mounted and read on first boot. At the minimum, the Day 0 configuration file must contain commands that will activate the management interface and set up the SSH server for public key authentication, but it can also contain a complete ASA configuration. The day0.iso file (either your custom day0.iso or the default day0.iso) must be available during first boot.

**Note**: To automatically license the ASAv during initial deployment, place the Smart Licensing Identity (ID) Token that you downloaded from the Cisco Smart Software Manager in a text file named ‘idtoken’ in the same directory as the Day 0 configuration file.

**Note**: If you want to deploy the ASAv in transparent mode, you must use a known running ASA config file in transparent mode as the Day 0 configuration file. This does not apply to a Day 0 configuration file for a routed firewall.

**Note**: We are using Linux in this example, but there are similar utilities for Windows.

### Procedure

1. Enter the CLI configuration for the ASAv in a text file called “day0-config”. Add interface configurations for the three interfaces and any other configuration you want.

   The fist line should begin with the ASA version. The day0-config should be a valid ASA configuration. The best way to generate the day0-config is to copy the desired parts of a running config from an existing ASA or ASAv. The order of the lines in the day0-config is important and should match the order seen in an existing show run command output.

   Example:

   ```
   ASA Version 9.4.1
   !
   interface management0/0
      nameif management
      security-level 100
      ip address 192.168.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/0
      nameif inside
      security-level 100
      ip address 10.1.1.2 255.255.255.0
      no shutdown
   interface gigabitethernet0/1
      nameif outside
      security-level 0
      ip address 198.51.100.2 255.255.255.0
      no shutdown
   http server enable
   http 192.168.1.0 255.255.255.0 management
   crypto key generate rsa modulus 1024
   username AdminUser password paSSw0rd
   ssh 192.168.1.0 255.255.255.0 management
   aaa authentication ssh console LOCAL
   ```

2. (Optional) Download the Smart License identity token file issued by the Cisco Smart Software Manager to your computer.

3. (Optional) Copy the ID token from the download file and put it a text file named ‘idtoken’ that only contains the ID token.

4. (Optional) For automated licensing during initial ASAv deployment, make sure the following information is in the day0-config file:

   - Management interface IP address
   - (Optional) HTTP proxy to use for Smart Licensing
   - A **route** command that enables connectivity to the HTTP proxy (if specified) or to tools.cisco.com
   - A DNS server that resolves tools.cisco.com to an IP address
   - Smart Licensing configuration specifying the ASAv license you are requesting
   - (Optional) A unique host name to make the ASAv easier to find in CSSM

5. Generate the virtual CD-ROM by converting the text file to an ISO file:

   ```
   stack@user-ubuntu:-/KvmAsa$ sudo genisoimage -r -o day0.iso day0-config idtoken
   I: input-charset not specified, using utf-8 (detected in locale settings)
   Total translation table size: 0
   Total rockridge attributes bytes: 252
   Total directory bytes: 0
   Path table size (byptes): 10
   ```

```
Max brk space used 0
176 extents written (0 MB)
stack@user-ubuntu:-/KvmAsa$
```

The Identity Token automatically registers the ASAv with the Smart Licensing server.

6. Repeat Steps 1 through 5 to create separate default configuration files with the appropriate IP addresses for each ASAv you want to deploy.

# Prepare the Virtual Bridge XML Files

You need to set up virtual networks that connect the ASAv guests to the KVM host and that connect the guests to each other.

**Note:** This procedure does not establish connectivity to the external world outside the KVM host.

Prepare the virtual bridge XML files on the KVM host. For the sample virtual network topology described in Prepare the Day 0 Configuration File, page 16, you need the following three virtual bridge files: virbr1.xml, virbr2.xml, and virbr3.xml (you must use these three filenames; for example, virbr0 is not allowed because it already exists). Each file has the information needed to set up the virtual bridges. You must give the virtual bridge a name and a unique MAC address. Providing an IP address is optional.

### Procedure

1. Create three virtual networks bridge XML files:

   virbr1.xml:

```
<network>
  <name>virbr1</name>
  <bridge name='virbr1' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:00' />
  <ip address='192.168.1.10' netmask='255.255.255.0' />
</network>
```

   virbr2.xml:

```
<network>
  <name>virbr2</name>
  <bridge name='virbr2' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:01' />
  <ip address='10.1.1.10' netmask='255.255.255.0' />
</network>
```

   virbr3.xml:

```
<network>
  <name>virbr3</name>
  <bridge name='virbr3' stp='on' delay='0' />
  <mac address='52:54:00:05:6e:02' />
  <ip address='198.51.100.10' netmask='255.255.255.0' />
</network>
```

2. Create a script that contains the following (in our example, we will name the script virt_network_setup.sh):

```
virsh net-create virbr1.xml
virsh net-create virbr2.xml
virsh net-create virbr3.xml
```

3. Run this script to setup the virtual network. The script brings the virtual networks up. The networks stay up as long as the KVM host is running.

```
stack@user-ubuntu:-/KvmAsa$ virt_network_setup.sh
```

**Note:** If you reload the Linux host, you must re-run the virt_network_setup.sh script. It does not persist over reboots.

4. Verify that the virtual networks were created:

```
stack@user-ubuntu:-/KvmAsa$ brctl show
bridge name     bridge id               STP enabled     Interfaces
virbr0          8000.0000000000000      yes
virbr1          8000.5254000056eed      yes             virb1-nic
virbr2          8000.5254000056eee      yes             virb2-nic
virbr3          8000.5254000056eec      yes             virb3-nic
stack@user-ubuntu:-/KvmAsa$
```

5. Display the IP address assigned to the virbr1 bridge. This is the IP address that you assigned in the XML file.

```
stack@user-ubuntu:-/KvmAsa$ ip address show virbr1
S: virbr1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 52:54:00:05:6e:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global virbr1
      valid_lft forever preferred_lft forever
```

# Launch the ASAv

Use a virt-install based deployment script to launch the ASAv.

### Procedure

1. Create a virt-install script called “virt_install_asav.sh”.

   The name of the ASAv VM must be unique across all other virtual machines (VMs) on this KVM host. The ASAv can support up to 10 networks. This example uses three networks. The order of the network bridge clauses is important. The first one listed is always the management interface of the ASAv (Management 0/0), the second one listed is GigabitEthernet 0/0 of the ASAv, and the third one listed is GigabitEthernet 0/1 of the ASAv, and so on up through GigabitEthernet0/8. The virtual NIC must be Virtio.

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=asav \
   --cpu host \
   --arch=x86_64 \
   --machine=pc-1.0 \
   --vcpus=1 \
   --ram=2048 \
   --os-type=linux \
   --os-variant=generic26 \
   --noacpi \
   --virt-type=kvm \
   --import \
   --disk path=/home/kvmperf/Images/desmo.qcow2,format=qcow2,device=disk,bus=ide,cache=none \
   --disk path=/home/kvmperf/asav_day0.iso,format=iso,device=cdrom \
   --console pty,target_type=virtio \
   --serial tcp,host=127.0.0.1:4554,mode=bind,protocol=telnet
```

2. Run the virt_install script:

```
stack@user-ubuntu:-/KvmAsa$ ./virt_install_asav.sh

Starting install...
Creating domain...
```

A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting you can issue CLI commands from the console screen.

# Deploy the ASAv On the AWS Cloud

You can deploy the ASAv on the Amazon Web Sources (AWS) cloud.



## About ASAv Deployment On the AWS Cloud

AWS is a public cloud environment that uses a private Xen Hypervisor. The ASAv runs as a guest in the AWS environment of the Xen Hypervisor. ASAv on AWS supports the following instance types:

- c3.large—2 vCPUs, 3.75 GB, 2 interfaces, 1 management interface

  **Note:** Both the ASAv10 and ASAv30 are supported on c3.large, but we do not recommend the ASAv30 on c3.large due to resource under-provisioning.

- c3.xlarge—4 vCPUs, 7.5 GB, 3 interfaces, 1 management interface

  **Note:** Only the ASAv30 is supported on c3.xlarge.

**Note:** The ASAv does not support the Xen Hypervisor outside of the AWS environment.

You create an account on AWS, set up the ASAv using the AWS Wizard, and chose an Amazon Machine Image (AMI). The AMI is a template that contains the software configuration needed to launch your instance.

**Note:** The AMI images are not available for download outside of the AWS environment.

## Prerequisites for the ASAv and AWS

- Create an account on aws.amazon.com.
- 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 Smart Software Licensing for the ASAv.
- 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 when using the c3.xlarge interface.
- For ASAv system requirements, see Cisco ASA Compatibility.

# Guidelines and Limitations for the ASAv and AWS

The ASAv on AWS supports the following features:

- Deployment in the Virtual Private Cloud (VPC)
- Enhanced networking (SR-IOV) where available
- Deployment from Amazon Marketplace
- Maximum of four vCPUs per instance
- User deployment of L3 networks
- Routed mode (default)

The ASAv on AWS does not support the following:

- Console access (management is performed using SSH or ASDM over network interfaces)
- IPv6
- VLAN
- Promiscuous mode (no sniffing or transparent mode firewall support)
- Multi-context mode
- Clustering
- ASAv native HA
- EtherChannel is only supported on direct physical interfaces
- VM import/export
- Amazon Cloudwatch
- Hypervisor agnostic packaging
- VMware ESXi
- Broadcast/multicast messages

  These messages are not propagated within AWS so routing protocols that require broadcast/multicast do not function as expected in AWS. VXLAN can operate only with static peers.

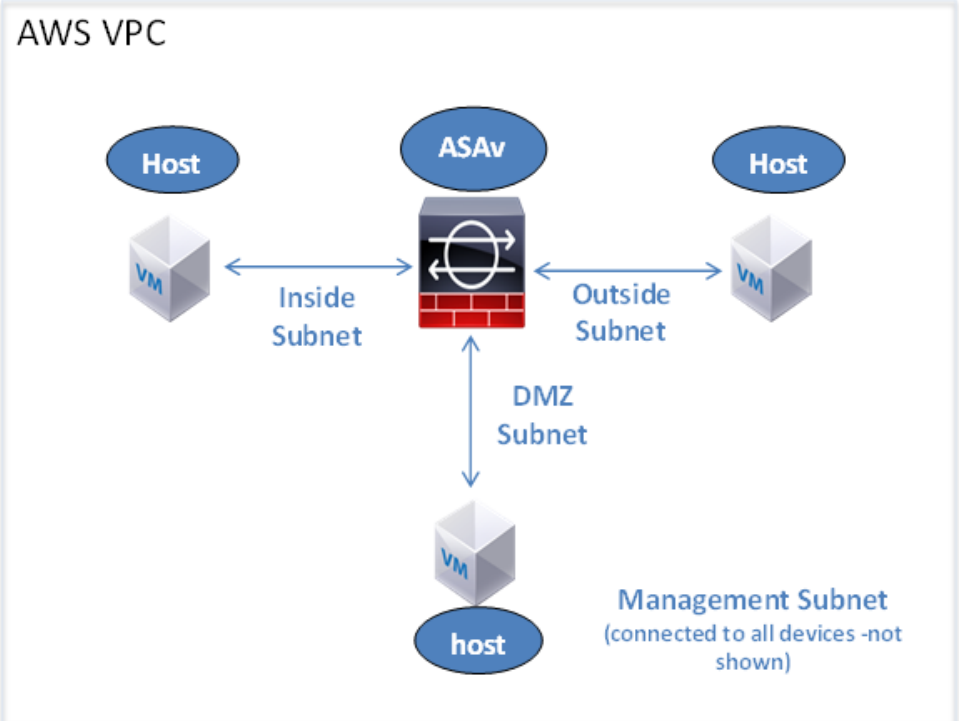
- Gratuitous/unsolicited ARPs

  These ARPS are not accepted within AWS so NAT configurations that require gratuitous ARPs or unsolicited ARPs do not function as expected.

# Sample Network Topology for ASAv on AWS

Figure 1 on page -23 shows the recommended topology for the ASAv in Routed Firewall Mode with four subnets configured in AWS for the ASAv (management, inside, outside, and DMZ).

**Figure 1 Sample ASAv on AWS Deployment**




# Deploy the ASAv on AWS

The following procedure is a top-level list of steps to set up AWS on the ASAv. For detailed steps for setup, see Getting Started with AWS.

**Procedure**

1. Log into aws.amazon.com and choose your region.

   AWS 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.

2. Click **My Account > AWS Management Console**, and under Networking, click **VPC > Start VPC Wizard**, and create your VPC by choosing a single public subnet, and set up the following (you can use the default settings unless otherwise noted):

   - Inside and outside subnet—Enter a name for the VPC and the subnets.
   - Internet Gateway—Enables direct connectivity over the Internet (enter the name of the Internet gateway).
   - outside table—Add entry to enable outbound traffic to the Internet (add 0.0.0.0/0 to Internet Gateway).

3. Click **My Account > AWS Management Console > EC2**, and then click **Create an Instance**.
   - Select your AMI (for example Ubuntu Server 14.04 LTS).

     Use the AMI identified in the your image delivery notification.
   - Choose the instance type supported by the ASAv (for example, c3.large).
   - Configure the instance (CPUs and memory are fixed).
   - Under Advanced Details, add the Day 0 Configuration if desired. For more information on how to configure the Day 0 configuration with more information, such as Smart Licensing, see Prepare the Day 0 Configuration File, page 16.

     Sample Day 0 Configuration

     ```
     ! ASA Version 9.4.1.200
     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 30
     username admin nopassword privilege 15
     username admin attributes
     service-type admin
     ! required config end
     ! example dns configuration
     dns domain-lookup management
     DNS server-group DefaultDNS
     ! where this address is the .2 on your public subnet
     name-server 172.19.0.2
     ! example ntp configuration
     name 129.6.15.28 time-a.nist.gov
     name 129.6.15.29 time-b.nist.gov
     name 129.6.15.30 time-c.nist.gov
     ntp server time-c.nist.gov
     ntp server time-b.nist.gov
     ntp server time-a.nist.gov
     ```
   - Storage (accept the defaults).
   - Tag Instance—You can create a lot of tags to classify your devices. Give it a name you can use to find it easily.
   - Security Group—Create a security group and name it. The security group is a virtual firewall for an instance to control inbound and outbound traffic.

     By default the Security Group is open to all addresses. Change the rules to only allow SSH in from addresses you will be using to access your ASAv.
   - Review your configuration and then click **Launch**.
4. Create a Key Pair.

   Give the key pair a name you will recognize and download the key to a safe place; the key can never be downloaded again. If you lose the key pair, you must destroy your instances and redeploy them again.
5. Click **Launch Instance** to deploy your ASAv.
6. Click **My Account > AWS Management Console > EC2 > Launch an Instance > My AMIs**.

7. Make sure that the Source/Destination Check is disabled per interface for the ASAv.

   AWS default settings only allow an instance to receive traffic for its IP address and only allow an instance to send traffic from its own IP address. To enable the ASAv to act as a routed hop, you must disable the Source/Destination Check on each of the ASAv's traffic interfaces (inside, outside, and DMZ).

# Configure the ASAv

The ASAv deployment pre-configures ASDM access. From the client IP address you specified during deployment, you can connect to the ASAv management IP address with a web browser. This chapter also describes how to allow other clients to access ASDM and also how to allow CLI access (SSH or Telnet). Other essential configuration tasks covered in this chapter include the license installation and common configuration tasks provided by wizards in ASDM.



## Start ASDM

**Procedure**

1. On the PC that you specified as the ASDM client, enter the following URL:

   **https://***asa_ip_address***/admin**

   The ASDM launch page appears with the following buttons:

   - **Install ASDM Launcher and Run ASDM**
   - **Run ASDM**
   - **Run Startup Wizard**

2. To download the Launcher:

   a. Click **Install ASDM Launcher and Run ASDM**.

   b. Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. Note: If you enabled HTTPS authentication, enter your username and associated password.

   c. Save the installer to your PC, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

   d. Enter the management IP address, leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

3. To use Java Web Start:

   a. Click **Run ASDM** or **Run Startup Wizard**.

   b. Save the shortcut to your PC when prompted. You can optionally open it instead of saving it.

   c. Start Java Web Start from the shortcut.

   d. Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

e. Leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

# Perform Initial Configuration Using ASDM

You can perform initial configuration using the following ASDM wizards and procedures. For CLI configuration, see the CLI configuration guides.



## Run the Startup Wizard

Run the **Startup Wizard** (choose **Wizards > Startup Wizard)** so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...

## (Optional) Allow Access to Public Servers Behind the ASAv

The **Configuration** > **Firewall** > **Public Servers** pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASAv, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.

## (Optional) Run VPN Wizards

You can configure VPN using the following wizards (**Wizards** > **VPN Wizards)**:

- Site-to-Site VPN Wizard—Creates an IPsec site-to-site tunnel between two ASAvs.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. The ASA policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- Clientless SSL VPN Wizard—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. ACLs can be applied to restrict or allow access to specific corporate resources.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard—Configures IPsec VPN remote access for the Cisco IPsec client.

## (Optional) Run Other Wizards in ASDM

- High Availability and Scalability Wizard—Configure failover or VPN load balancing.
- Packet Capture Wizard—Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

# Advanced Configuration

To continue configuring your ASAv, see Navigating the Cisco ASA Series Documentation.