Deploy the ASAv On the Microsoft Azure Cloud

You can deploy the ASAv on the Microsoft Azure cloud.

About ASAv Deployment On the Microsoft Azure Cloud

Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. The ASAv runs as a guest in the Microsoft Azure environment of the Hyper V Hypervisor. The ASAv on Microsoft Azure supports the Standard D3 and Standard D3_v2 instances, which supports four vCPUs, 14 GB, and four interfaces.

You can deploy the ASAv on Microsoft Azure in one of three ways:

- As a stand-alone firewall using the Azure Resource Manager
- As an integrated partner solution using the Azure Security Center
- As a high availability (HA) pair using the Azure Resource Manager

See Deploy the ASAv on Microsoft Azure, page 56. Note that you can only deploy the ASAv HA configuration using the Azure Resource Manager.

Prerequisites and System Requirements for the ASAv and Azure

- Create an account on Azure.com.

  After you create an account on Microsoft Azure, you can log in, choose the ASAv in the Microsoft Azure Marketplace, and deploy the ASAv.

- 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.

  Note: The ASAv defaults to the ASAv30 entitlement when deployed on Azure. The use of the ASAv5 and ASAv10 entitlement is allowed. However, the throughput level must be explicitly configured to use the ASAv5 or ASAv10 entitlement.

- Interface requirements:

  You must deploy the ASAv with four interfaces on four networks.

  - Management interface

    Note: For edge firewall configurations, the Management interface is also used as the “outside” interface.

    Note: In Azure, the first defined interface, which is always the Management interface, is the only interface that can have an Azure public IP address associated with it. Because of this, the ASAv in Azure allows though-data traffic on the Management interface. Therefore the initial configuration for the Management interface does not include the **management-only** setting.

  - Inside and outside interfaces
  - Additional subnet (DMZ or any network you choose)

- Communications paths:
  - Management interface–Used for SSH access and to connect the ASAv to the ASDM.
  - 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 Standard_D3 interface.

- For ASAv system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations for the ASAv and Azure

Supported Features

- Deployment from Microsoft Azure Cloud
- Maximum of four vCPUs per instance
- User deployment of L3 networks

  Note: Azure does not provide configurable L2 vSwitch capability.

- Routed firewall mode (default)

  Note: In routed firewall mode the ASAv is a traditional Layer 3 boundary in the network. This mode requires an IP address for each interface. Because Azure does not support VLAN tagged interfaces, the IP addresses must be configured on non-tagged, non-trunk interfaces.

- ASAv HA (single context mode)

Note: If your deployment uses an Azure Load Balancer, health probes are not supported on secondary IP addresses assigned on ASAv NICs.

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- IPv6
- VLAN tagging on user instance interfaces
- Jumbo frames
- Proxy ARP for an IP address that the device does not own from an Azure perspective
- Public IP address on any interface

  Only the Management 0/0 interface can have a public IP address associated with it.
- Promiscuous mode (no sniffing or transparent mode firewall support)

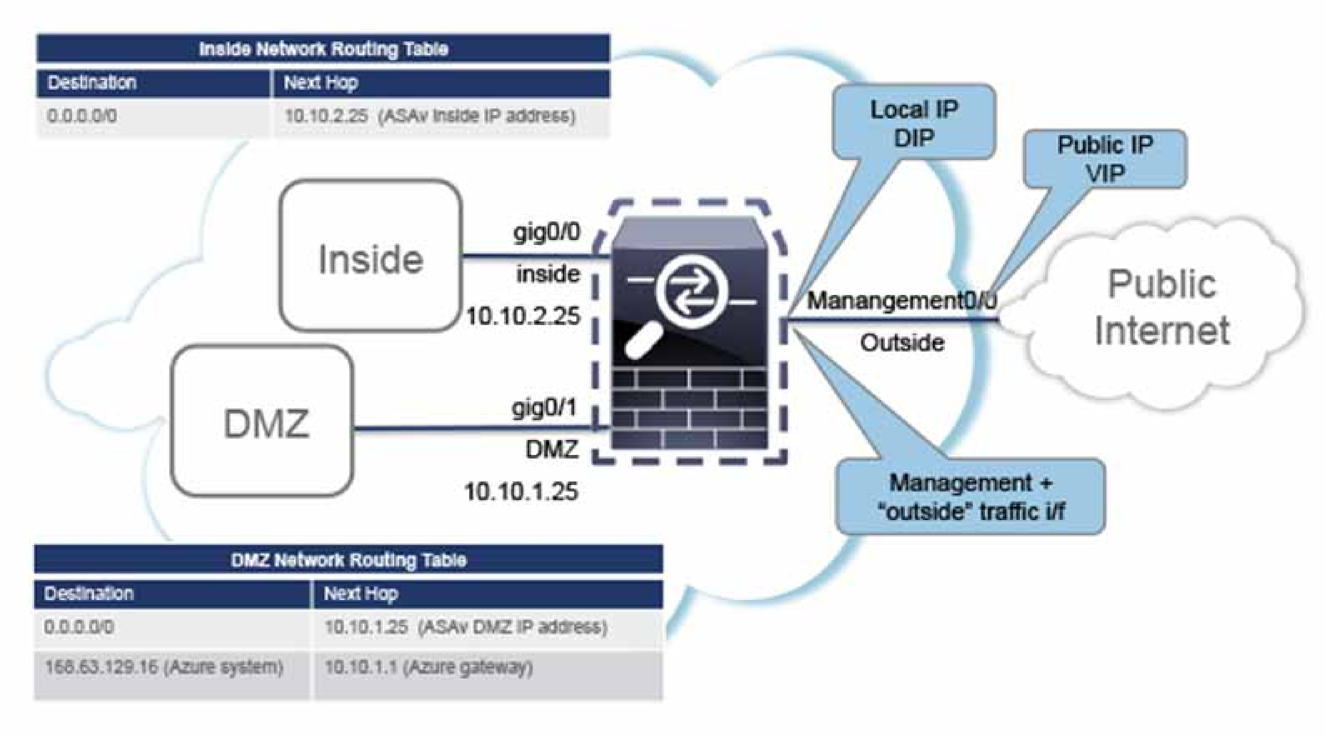
  Note: Azure policy prevents the ASAv from operating in transparent firewall mode because it doesn't allow interfaces to operate in promiscuous mode.
- Multi-context mode
- Clustering
- VM import/export
- By default, FIPS mode is not enabled on the ASAv running in the Azure cloud.

  Caution: If you enable FIPS mode, you must change the Diffie-Helman key exchange group to a stronger key by using the **ssh key-exchange group dh-group14-sha1** command. If you don’t change the Diffie-Helman group, you will no longer be able to SSH to the ASAv, and that is the only way to initially manage the ASAv.

Sample Network Topology for ASAv on Azure

Figure 1 on page -54 shows the recommended topology for the ASAv in Routed Firewall Mode with three subnets configured in Azure (management, inside, DMZ). The fourth required interface (outside) is not shown.

Figure 1 Sample ASAv on Azure Deployment



Inside Network Routing Table

Destination	Next Hop
0.0.0.0/0	10.10.2.25 (ASAv inside IP address)

DMZ Network Routing Table

Destination	Next Hop
0.0.0.0/0	10.10.1.25 (ASAv DMZ IP address)
168.63.129.16 (Azure system)	10.10.1.1 (Azure gateway)

Resources Created During Deployment

When you deploy the ASAv in Azure the following resources are created:

- The ASAv Virtual Machine (VM)
- A resource group (unless you chose an existing resource group)

  The ASAv resource group must be the same resource group used by the Virtual Network and the Storage Account.
- Four NICS named *vm name*-Nic0, *vm name*-Nic1, *vm name*-Nic2, *vm name*-Nic3

  These NICs map to the ASAv interfaces Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, and GigabitEthernet 0/2 respectively.
- A security group named *vm name*-SSH-SecurityGroup

  The security group will be attached to the VM's Nic0, which maps to ASAv Management 0/0.

  The security group includes rules to allow SSH and UDP ports 500 and UDP 4500 for VPN purposes. You can modify these values after deployment.
- A Public IP Address (named according to the value you chose during deployment)

  The public IP address is associated with VM Nic0, which maps to Management 0/0. Azure only allows a public IP address to be associated with the first NIC.

Note: You must choose a public IP address (new or existing); the NONE option is not supported.

- A Virtual Network with four subnets (unless you chose an existing network)
- A Routing Table for each subnet (updated if it already exists)

  The tables are named *subnet name*-ASAv-RouteTable.

  Each routing table includes routes to the other three subnets with the ASAv IP address as the next hop. You may chose to add a default route if traffic needs to reach other subnets or the Internet.

- A boot diagnostics file in the selected storage account

  The boot diagnostics file will be in Blobs (binary large objects).

- Two files in the selected storage account under Blobs and container VHDs named *vm name*-disk.vhd and *vm name*-<uuid>.status
- A Storage account (unless you chose an existing storage account)

  Note: When you delete a VM, you must delete each of these resources individually, except for any resources you want to keep.

Azure Routing

Routing in an Azure Virtual Network is determined by the Virtual Network's Effective Routing Table. The Effective Routing Table is a combination of an existing System Routing Table and the User Defined Routing Table.

Note: Currently you cannot view either the Effective Routing Table or the System Routing Table.

You can view and edit the User Defined Routing table. When the System table and the User Defined tables are combined to form the Effective Routing Table, the most specific route wins and ties go to the User Defined Routing table. The System Routing Table includes a default route (0.0.0.0/0) pointing to Azure's Virtual Network Internet Gateway. The System Routing Table also includes specific routes to the other defined subnets with the next-hop pointing to Azure's Virtual Network infrastructure gateway.

To route traffic through the ASAv, the ASAv deployment process adds routes on each subnet to the other three subnets using the ASAv as the next hop. You may also want to add a default route (0.0.0.0/0) that points to the ASAv interface on the subnet. This will send all traffic from the subnet through the ASAv, which may require that ASAv policies be configured in advance to handle that traffic (perhaps using NAT/PAT).

Because of the existing specific routes in the System Routing Table, you must add specific routes to the User Defined Routing table to point to the ASAv as the next-hop. Otherwise, a default route in the User Defined table would lose to the more specific route in the System Routing Table and traffic would bypass the ASAv.

Routing Configuration for VMs in the Virtual Network

Routing in the Azure Virtual Network depends on the Effective Routing Table and not the particular gateway settings on the clients. Clients running in a Virtual Network may be given routes by DHCP that are the .1 address on their respective subnets. This is a place holder and serves only to get the packet to the Virtual Network's infrastructure virtual gateway. Once a packet leaves the VM it is routed according to the Effective Routing Table (as modified by the User Defined Table). The Effective Routing Table determines the next hop regardless of whether a client has a gateway configured as .1 or as the ASAv address.

Azure VM ARP tables will show the same MAC address (1234.5678.9abc) for all known hosts. This ensures that all packets leaving an Azure VM will reach the Azure gateway where the Effective Routing Table will be used to determine the path of the packet.

IP Addresses

The following information applies to IP addresses in Azure:

- You should use DHCP to set the IP addresses of ASAv interfaces. Furthermore, Management 0/0 (which maps to the first NIC on the ASAv) **is required** to use DHCP to obtain its IP address.

  The Azure infrastructure ensures that the ASAv interfaces are assigned the IP addresses set in Azure.
- Management 0/0 is given a private IP address in the subnet to which it was attached.

  A public IP address may be associated with this private IP address and the Azure Internet gateway will handle the NAT translations.
- Only the first NIC on a VM may have a public IP address attached.
- Public IP addresses that are dynamic may change during an Azure stop/start cycle. However, they are persistent during Azure restart and during ASAv reload.
- Public IP addresses that are static won't change until you change them in Azure.
- If you have an HA deployment that uses an Azure Load Balancer, health probes are not supported on secondary IP addresses assigned on ASAv NICs.

DNS

All Azure virtual networks have access to a built-in DNS server at 168.63.129.16 that you can use as follows:

```
configure terminal
dns domain-lookup management
dns server-group DefaultDNS
 name-server 168.63.129.16
end
```

You can use this configuration when you configure Smart Licensing and you don’t have your own DNS Server set up.

Deploy the ASAv on Microsoft Azure

You can deploy the ASAv on Microsoft Azure in one of two ways:

- Deploy the ASAv as a stand-alone firewall using the Azure Resource Manager. See Deploy the ASAv from Azure Resource Manager, page 56.
- Deploy the ASAv as an integrated partner solution within Azure using the Azure Security Center. Security-conscious customers are offered the ASAv as a firewall option to protect Azure workloads. Security and health events are monitored from a single integrated dashboard. See Deploy the ASAv from Azure Security Center, page 58.
- Deploy an ASAv High Availablity pair using the Azure Resource Manager. See Deploy ASAv for High Availability from Azure Resource Manager, page 60.

Deploy the ASAv from Azure Resource Manager

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

When you deploy the ASAv in Azure it automatically generates various configurations, such as resources, public IP addresses, and route tables. You can further manage these configurations after deployment. For example, you may want to change the Idle Timeout value from the default, which is a low timeout.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. Search Marketplace for Cisco ASAv, and then click on the ASAv you would like to deploy.

3. Configure the basic settings.

   a. Enter a name for the virtual machine. This name should be unique within your Azure subscription.

      Note: Make sure you do not use an existing name or the deployment will fail.

   b. Enter your username.

   c. Choose an authorization type either password or SSH key.

      If you choose password, enter a password and confirm.

   d. Choose your subscription type.

   e. Choose a resource group.

      The resource group should be the same as the virtual network's resource group.

   f. Choose your location.

      The location should be the same as for your network and resource group.

   g. Click **OK**.

4. Configure the ASAv settings.

   a. Choose the virtual machine size.

      Note: The only size available for the ASAv is Standard D3.

   b. Choose a storage account.

      Note: You can use an existing storage account or create a new one. The location of the storage account should be the same as for the network and virtual machine.

   c. Request a public IP address by entering a label for the IP address in the Name field, and then click **OK**.

      Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

   d. Add a DNS label if desired.

      Note: The fully qualified domain name will be your DNS label plus the Azure URL:
      <dnslabel>.<location>.cloupapp.azure.com

   e. Choose an existing virtual network or create a new one.

   f. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Note: Each interface must be attached to a unique subnet.

g. Click **OK**.

5. View the configuration summary, and then click **OK**.

6. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page 77 for instructions for accessing the ASDM.

Deploy the ASAv from Azure Security Center

The Microsoft Azure Security Center is a security solution for Azure that enables customers to protect, detect, and mitigate security risks for their cloud deployments. From the Security Center dashboard, customers can set security policies, monitor security configurations, and view security alerts.

Security Center analyzes the security state of Azure resources to identify potential security vulnerabilities. A list of recommendations guides customers through the process of configuring needed controls, which can include deployment of the ASAv as a firewall solution to Azure customers.

As an integrated solution in Security Center, you can rapidly deploy the ASAv in just a few clicks and then monitor security and health events from a single dashboard. The following procedure is a top-level list of steps to deploy the ASAv from Security Center. For more detailed information, see Azure Security Center.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. From the Microsoft Azure menu, choose **Security Center**.

   If you are accessing Security Center for the first time, the **Welcome** blade opens. Choose **Yes! I want to Launch Azure Security Center** to open the **Security Center** blade and to enable data collection.

3. On the **Security Center** blade, select the **Policy** tile.

4. On the **Security policy** blade, choose **Prevention policy**.

5. On the **Prevention policy** blade, turn on the recommendations that you want to see as part of your security policy.

   a. Set **Next generation firewall** to **On**. This ensures that the ASAv is a recommended solution in Security Center.

   b. Set any other recommendations as needed.

6. Return to the **Security Center** blade and select the **Recommendations** tile.

   Security Center periodically analyzes the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it shows recommendations on the **Recommendations** blade.

7. Select the **Add a Next Generation Firewall** recommendation on the **Recommendations** blade to view more information and/or to take action to resolve the issue.

8. Choose **Create New** or **Use existing solution**, and then click on the ASAv you would like to deploy.

9. Configure the basic settings.

   c. Enter a name for the virtual machine. This name should be unique within your Azure subscription.

Note: Make sure you do not use an existing name or the deployment will fail.

d. Enter your username.

e. Choose an authorization type either password or SSH key.

If you choose password, enter a password and confirm.

f. Choose your subscription type.

g. Choose a resource group.

The resource group should be the same as the virtual network's resource group.

h. Choose your location.

The location should be the same as for your network and resource group.

i. Click **OK**.

10. Configure the ASAv settings.

a. Choose the virtual machine size.

Note: The only size available for the ASAv is Standard D3.

b. Choose a storage account.

Note: You can use an existing storage account or create a new one. The location of the storage account should be the same as for the network and virtual machine.

c. Request a public IP address by entering a label for the IP address in the Name field, and then click **OK**.

Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

d. Add a DNS label if desired.

Note: The fully qualified domain name will be your DNS label plus the Azure URL:
<dnslabel>.<location>.cloupapp.azure.com

e. Choose an existing virtual network or create a new one.

f. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

Note: Each interface must be attached to a unique subnet.

g. Click **OK**.

11. View the configuration summary, and then click **OK**.

12. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page 77 for instructions for accessing the ASDM.
- If you need more information on how the recommendations in Security Center help you protect your Azure resources, see the documentation available from Security Center.

Deploy ASAv for High Availability from Azure Resource Manager

The following procedure is a top-level list of steps to set up a High Availability (HA) ASAv pair on Microsoft Azure. For detailed steps for Azure setup, see Getting Started with Azure.

ASAv HA in Azure deploys two ASAvs into an Availability Set, and automatically generates various configurations, such as resources, public IP addresses, and route tables. You can further manage these configurations after deployment.

Procedure

1. Log into the Azure portal.

   The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

2. Search Marketplace for **Cisco ASAv**, and then click on the **ASAv 4 NIC HA** to deploy a failover ASAv configuration.

3. Configure the **Basics** settings.

   h. Enter a prefix for the ASAv virtual machine names. The ASAv names will be **'prefix'-A** and **'prefix'-B**.

      Note: Make sure you do not use an existing prefix or the deployment will fail.

   i. Enter a **Username**.

      Note: This will be the administrative username for both Virtual Machines. The username **admin** is not allowed in Azure.

   j. Choose an authentication type for both Virtual Machines, either **Password** or **SSH public key**.

      If you choose **Password**, enter a password and confirm.

   k. Choose your subscription type.

   l. Choose a **Resource group**.

      Choose **Create new** to create a new resource group, or **Use existing** to select an existing resource group. If you use an existing resource group, it must be empty. Otherwise you should create a new resource group.

   m. Choose your **Location**.

      The location should be the same as for your network and resource group.

   n. Click **OK**.

4. Configure the **Cisco ASAv settings**.

   a. Choose the Virtual Machine size.

      Note: The only size available for the ASAv HA is Standard D3 v2.

   b. Choose **Managed** or **Unmanaged OS disk** storage.

      Note: ASA HA mode always uses **Managed**.

5. Configure the **ASAv-A** settings.

   a. (Optional) Choose **Create new** to request a public IP address by entering a label for the IP address in the Name field, and then click **OK**. Choose **None** if you do not want a public IP address.

      Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

b. Add a DNS label if desired.

   Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

c. Configure the required settings for the storage account for the ASAv-A boot diagnostics.

6. Configure the **ASAv-B** settings.

   a. (Optional) Choose **Create new** to request a public IP address by entering a label for the IP address in the Name field, and then click **OK**. Choose **None** if you do not want a public IP address.

      Note: Azure creates a dynamic public IP by default, which may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can open the public-ip in the portal and change it from a dynamic to a static address.

   b. Add a DNS label if desired.

      Note: The fully qualified domain name will be your DNS label plus the Azure URL: <dnslabel>.<location>.cloupapp.azure.com

   c. Configure the required settings for the storage account for the ASAv-B boot diagnostics.

7. Choose an existing virtual network or create a new one.

   d. Configure the four subnets that the ASAv will deploy to, and then click **OK**.

      Note: Each interface must be attached to a unique subnet.

   e. Click **OK**.

8. View the **Summary** configuration, and then click **OK**.

9. View the terms of use and then click **Create**.

What to Do Next

- Continue configuration using CLI commands available for input via SSH. See the *ASA Configuration Guide* chapter “Failover for High Availability in the Public Cloud” for more information.