Deploy the ASA Virtual on Azure

You can deploy the ASA Virtual on the Microsoft Azure cloud.

Important Beginning with 9.13(1), any ASA Virtual license now can be used on any supported ASA Virtual vCPU/memory configuration. This allows the ASA Virtual customers to run on a wide variety of VM resource footprints. This also increases the number of supported Azure instances types.

Important Beginning with 9.13(1), any ASA Virtual license now can be used on any supported ASA Virtual vCPU/memory configuration. This allows the ASA Virtual customers to run on a wide variety of VM resource footprints. This also increases the number of supported Azure instances types.

Overview

Select the Azure virtual machine (VM) tier and size to meet your ASA Virtual needs. Any ASA Virtual license can be used on any supported ASA Virtual vCPU/memory configuration. This allows you to run the ASA Virtual on a wide variety of Azure VM sizes.

Azure Supported VM Sizes

Table 1: Azure Supported VM Sizes and ASA Virtual Versions

Azure VM Size	Attributes		vNICs	ASA Virtual Version
	vCPUs	Memory (GB)		
Standard_D3	4	14	4	9.23 or later
Standard_D3_v2	4	14	4	9.23 or later
Standard_DS3	4	14	4	9.13 or later
Standard_DS3_v2	4	14	4	9.13 or later
Standard_D4	8	28	8	9.13 or later
Standard_D4_v2	8	28	8	9.13 to 9.23
Standard_DS4	8	28	8	9.13 or later
Standard_DS4_v2	8	28	8	9.13 or later
Standard_D5_v2	16	56	8	9.13 to 9.23
Standard_DS5_v2	16	56	8	9.15.1 or later
Standard_D8_v3	8	32	4	9.13 or later
Standard_D16_v3	16	64	8	9.15.1 or later
Standard_D8s_v3	8	32	4	9.17.1 or later
Standard_D16s_v3	16	64	8	9.17.1 or later
Standard_D8s_v5	8	32	8	9.23.1 or later
Standard_D16s_v5	16	64	8	9.23.1 or later
Standard_F4	4	8	4	9.13 or later
Standard_F4s	4	8	4	9.13 or later
Standard_F8	8	16	4	9.13 or later
Standard_F8s	8	16	4	9.13 or later
Standard_F16	16	32	4	9.15.1 or later
Standard_F16s	16	32	4	9.15.1 or later
Standard_F8s_v2	8	32	4	9.17.1 or later
Standard_F16s_v2	16	64	8	9.17.1 or later
Standard_D8_v4	8	32	4	9.23.1 or later

Azure VM Size	Attributes		vNICs	ASA Virtual Version
	vCPUs	Memory (GB)		
Standard_D16_v4	16	64	8	9.23.1 or later
Standard_D8s_v4	8	32	4	9.23.1 or later
Standard_D16s_v4	16	64	8	9.23.1 or later
Standard_D8_v5	8	32	4	9.23.1 or later
Standard_D16_v5	16	64	8	9.23.1 or later
Standard_D8s_v5	8	32	4	9.23.1 or later
Standard_D16s_v5	16	64	8	9.23.1 or later
Standard_D8s_v6	8	32	4	9.24.10 or later
Standard_D16s_v6	16	64	8	9.24.10 or later

Starting from ASA version 9.24.10, the following network-optimized Azure VM sizes are also supported.

VM size	vCPUs	Memory (GB)	Maximum number of interfaces	Supported version
Standard_D2ns_v6	2	8	4	9.24.10 and later
Standard_D4ns_v6	4	16	4	
Standard_D8ns_v6	8	32	8	
Standard_D16ns_v6	16	64	8	
Standard_D2nds_v6	2	8	4	
Standard_D4nds_v6	4	16	4	
Standard_D8nds_v6	8	32	8	
Standard_D16nds_v6	16	64	8	
Standard_D2nls_v6	2	4	4	
Standard_D4nls_v6	4	8	4	
Standard_D8nls_v6	8	16	8	
Standard_D16nls_v6	16	32	8	
Standard_D2nlds_v6	2	4	4	
Standard_D4nlds_v6	4	8	4	
Standard_D8nlds_v6	8	16	8	
Standard_D16nlds_v6	16	32	8	

Note The ASAv100 is not supported on Microsoft Azure.

Note

- By default, ASA Virtual instances are deployed with Secure Boot enabled.
- From 9.24.1 onwards, only the Gen-2 instance types are supported.
- ASA virtual maximum vCPU limit: ASA virtual supports a maximum of 16 vCPUs. Instances exceeding this capacity are not supported. ASAvU (ASAv-Unlimited) is supported only on KVM, VMware, and AWS.
- ASA virtual minimum vCPU requirement: ASA virtual requires a minimum of 4 vCPUs. Instances with fewer than 4 vCPUs are not supported.

Table 2: ASA Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	VM size (Core/RAM)	Rate Limit	RA VPN Session Limit
ASAv5	Standard_D3_v2 4 core/14 GB	100 Mbps	50
ASAv10	Standard_D3_v2 4 core/14 GB	1 Gbps	250
ASAv30	Standard_D3_v2 4 core/14 GB	2 Gbps	750
ASAv50	Standard_D4_v2 8 core/28 GB	5.5 Gbps	10,000
ASAv100	Standard_D5_v2 16 core/56 GB	11 Gbps	20,000

You can deploy the ASA Virtual on Microsoft Azure:

- As a stand-alone firewall using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments
- As an integrated partner solution using the Azure Security Center
- As a high availability (HA) pair using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments

Note In the event of unexpected failovers in a ASA Virtual HA setup, check the logs for any brief communication interruptions with peer ASA Virtual instances or Azure services. If such failover is observed, then it is advisable to configure a static IP address for the management interface instead of assigning IP address through DHCP.

See Deploy the ASA Virtual from Azure Resource Manager, on page 15. Note that you can deploy the ASA Virtual HA configuration on the standard Azure public cloud and the Azure Government environments.

Prerequisites

- Create an account on Azure.com.

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

- License the ASA Virtual.

Until you license the ASA Virtual, it will run in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Smart Software Licensing for the ASA Virtual.

Note The ASA Virtual defaults to the 2Gbps entitlement when deployed on Azure. The use of the 100Mbps and 1Gbps entitlement is allowed. However, the throughput level must be explicitly configured to use the 100Mbps or 1Gbps entitlement.

- Interface requirements:

  You must deploy the ASA Virtual with four interfaces on four networks. You can assign a public IP address to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

- Management interface:

  In Azure, the first defined interface is always the Management interface.

Note For IPv6 deployment, configure the IPv6 in the Vnet and subnet creation.

- Communications paths:
  - Management interface—Used for SSH access and to connect the ASA Virtual to the ASDM.

Note Azure accelerated networking is not supported on the Management interface.

  - Inside interface (required)—Used to connect the ASA Virtual to inside hosts.
  - Outside interface (required)—Used to connect the ASA Virtual to the public network.
  - DMZ interface (optional)—Used to connect the ASA Virtual to the DMZ network when using the Standard_D3 interface.

- For ASA Virtual hypervisor and virtual platform support information, see Cisco Secure Firewall ASA Compatibility.

Guidelines and Limitations

Supported Features

- Deployment from Microsoft Azure Cloud.
- Azure Accelerated Networking (AN)
- Maximum of 16 vCPUs, based on the selected VM size.

Note Azure does not provide configurable L2 vSwitch capability.

- Public IP address on any interface

  You can assign a public IP address to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

- Routed firewall mode (default)

Note In routed firewall mode the ASA Virtual 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.

- IPv6

Azure DDoS Protection Feature

Azure DDoS Protection in Microsoft Azure is an additional feature implemented at the forefront of ASA Virtual. In a virtual network, when this feature is enabled it helps to defend applications against common network layer attacks depending on the packet per second of a network's expected traffic. You can customize this feature based on the network traffic pattern.

For more information about the Azure DDoS Protection feature, see Azure DDoS Protection Standard overview.

Password Setup

Ensure that the password you set complies with the guidelines given below. The password must:

- Be an alphanumeric string with a minimum of 12 characters and a maximum of 72 characters
- Comprise of lowercase and uppercase characters, numbers, and special characters that are not '\' or '-'
- Have no more than 2 repeating or sequential ASCII characters
- Not be a word that can be found in the dictionary

If you observe any deployment issues, such as those listed below, or any other password-related errors in the boot logs, you should check whether your configured password complies with the password complexity guidelines.

Deployment Errors

- `OS Provisioning failed for VM 'TEST-CISCO-TDV-QC' due to an internal error. (Code: OSProvisioningInternal Error)`
- `OS Provisioning failed for VM 'TEST-CISCO-ASAVM' due to an internal error. InternalDetail: RoleInstanceContainerProvisioningDetails: MediaStorageAccountName:ProvisionVmWithUpdate; MediaStorageHostName:ProvisionVmWithUpdate; MediaRelativeUrl:ProvisionVmWithUpdate; MediaTenantSecretId:00000000-0000-0000-0000-000000000000; ProvisioningResult:Failure; ProvisioningResultMessage:[ProtocolError] [CopyOvfEnv]`

```
Error mounting dvd: [OSUtilError] Failed to mount dvd device Inner error: [mount -o ro
 -t udf,iso9660 /dev/hdc /mnt/cdrom/secure] returned 32:
mount: /mnt/cdrom/secure: no medium found on /dev/hdc
```

You can review and reconfirm these password-related errors by referring to the Serial console log. The following is an example of an error detail from a serial console log:

```
10150 bytes copied in 0.80 secs
Waagent - 2024-08-02T00:46:55.889400Z INFO Daemon Create user account if not exists
Waagent - 2024-08-02100:46:55.890685Z INFO Daemon Set user password.
ERROR: Password must contain:
ERROR: a value that has less than 3 repetitive or sequential ASCII characters.
Invalid Eg:aaaauser, user4321, aaabc789
Failed to add username "cisco"
ADD_USER reply indicates failure
```

Known Issues

Idle Timeout

The ASA Virtual on Azure has a configurable *idle timeout* on the VM. The minimum setting is 4 minutes and the maximum setting is 30 minutes. However, for SSH sessions the minimum setting is 5 minutes and the maximum setting is 60 minutes.

Note Be aware that the ASA Virtual's idle timeout always overrides the SSH timeout and disconnects the session. You can choose to match the VM's idle timeout to the SSH timeout so that the session does not timeout from either side.

Failover from Primary ASA Virtual to Standby ASA Virtual

When an Azure upgrade occurs on an ASA Virtual HA in Azure deployment, a failover may occur from the primary ASA Virtual to the standby ASA Virtual. An Azure upgrade causes the primary ASA Virtual to enter a pause state. The standby ASA Virtual does not receive any hello packets when the primary ASA Virtual is paused. If the standby ASA Virtual does not receive any hello packets beyond the failover hold time, a failover to the standby ASA Virtual occurs.

There is also the possibility of a failover occurring even if the failover hold time has not been exceeded. Consider a scenario in which the primary ASA Virtual resumes 19 seconds after entering the pause state. The failover hold time is 30 seconds. But, the standby ASA Virtual does not receive hello packets with the right timestamp because the clock is synchronized every ~2 minutes. This causes a failover from the primary ASA Virtual to the standby ASA Virtual.

Note This feature supports IPv4 only, ASA Virtual HA is not supported for IPv6 configuration.

Unsupported Features

- Console access (management is performed using SSH or ASDM over network interfaces)
- VLAN tagging on user instance interfaces
- Jumbo frames

- Proxy ARP for an IP address that the device does not own from an Azure perspective
- Promiscuous mode (no sniffing or transparent mode firewall support)

Note Azure policy prevents the ASA Virtual from operating in transparent firewall mode because it doesn't allow interfaces to operate in promiscuous mode.

- Multi-context mode
- Clustering
- ASA Virtual native HA.

Note You can deploy ASA Virtual on Azure in a stateless Active/Backup high availability (HA) configuration.

- VM import/export
- By default, FIPS mode is not enabled on the ASA Virtual running in the Azure cloud.

Note 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 ASA Virtual, and that is the only way to initially manage the ASA Virtual.

- Re-sizing the VM after deployment
- Migration or update of the Azure Storage SKU for the OS Disk of the VM from premium to standard SKU and vice versa

UEFI and Secure Boot Limitations

On Azure, UEFI firmware is supported only for greenfield (fresh) deployments and must be enabled during initial deployment.

Existing brownfield deployments can be upgraded to Version 9.24 without impact. Changing the boot mode or enabling UEFI Secure Boot after deployment is not supported.

Upgrade Restrictions and Limitations

Revert upgrade restrictions

Caution Reverting an upgrade is not supported.

Ensure that you take a backup before upgrading. After upgrading to ASA Virtual 9.24, you cannot roll back to a previous software version. To return to an earlier version, you must redeploy the Management Center.

Resources Created During Deployment

When you deploy the ASA Virtual in Azure the following resources are created:

- The ASA Virtual machine
- A resource group (unless you chose an existing resource group)

  The ASA Virtual 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 ASA Virtual interfaces Management 0/0, GigabitEthernet 0/0, GigabitEthernet 0/1, and GigabitEthernet 0/2 respectively.

Note Based on the requirement, you can create Vnet with IPv4 only or Dual Stack (IPv4 and IPv6 enabled).

- A security group named vm name-SSH-SecurityGroup

  The security group will be attached to the VM's Nic0, which maps to ASA Virtual 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.
- Public IP addresses (named according to the value you chose during deployment)

  You can assign a public IP address (IPv4 only or Dual Stack (Ipv4 and IPv6)).

  to any interface; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.
- 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 ASA Virtual 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 The ASA Virtual cannot use dynamic interior routing protocols like EIGRP and OSPF due to the nature of Azure cloud routing. The Effective Routing Table determines the next hop, regardless of whether a virtual client has any static/dynamic route configured.

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 ASA Virtual, the ASA Virtual deployment process adds routes on each subnet to the other three subnets using the ASA Virtual as the next hop. You may also want to add a default route (0.0.0.0/0) that points to the ASA Virtual interface on the subnet. This will send all traffic from the subnet through the ASA Virtual, which may require that ASA Virtual 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 ASA Virtual 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 ASA Virtual.

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 ASA Virtual 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.

Note The ASA Virtual cannot use dynamic interior routing protocols like EIGRP and OSPF due to the nature of Azure cloud routing. The Effective Routing Table determines the next hop, regardless of whether a virtual client has any static/dynamic route configured.

Note Virtual Networks, Subnets, Interface, etc., cannot be created by using IPv6 alone. The IPv4 is used by default, and IPv6 can be enabled along with it.

IP Addresses

The following information applies to IP addresses in Azure:

- You should use DHCP to set the IP addresses of ASA Virtual interfaces. Furthermore, Management 0/0 (which maps to the first NIC on the ASA Virtual) **is required** to use DHCP to obtain its IPv6 address.

  The Azure infrastructure ensures that the ASA Virtual interfaces are assigned the IP addresses set in Azure.

- Management 0/0 is given a private IP address in the subnet to which it is attached.

  A public IP address may be associated with this private IP address and the Azure Internet gateway will handle the NAT translations.

- You can assign a public IP address to any interface.
- You can enable **IP Forwarding** in the network interface attached to an ASA Virtual appliance in a Virtual Machine Scale Set (VMSS). If network traffic is not destined to any of the configured IP addresses in the network interface, then enabling this option forwards such network traffic to other IP addresses other than the IP addresses configured in the virtual machine. See Azure documentation on how to enable IP Forwarding in the network interface - Enable or disable IP forwarding.
- Public IP addresses that are dynamic may change during an Azure stop/start cycle. However, they are persistent during Azure restart and during ASA Virtual reload.
- Public IP addresses that are static won't change until you change them in Azure.

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.

Accelerated Networking (AN)

Azure's Accelerated Networking (AN) feature enables single root I/O virtualization (SR-IOV) to a VM, which accelerates networking by allowing VM NICs to bypass the hypervisor and go directly to the PCIe card underneath. AN significantly enhances the throughput performance of the VM and also scales with additional cores (i.e. larger VMs).

AN is disabled by default. Azure supports enabling AN on pre-provisioned virtual machines. You simply have to stop VM in Azure and update the network card property to set the *enableAcceleratedNetworking* parameter to true. See the Microsoft documentation Enable accelerated networking on existing VMs. Then restart the VM.

Support for Mellanox Hardware

Microsoft Azure cloud has two types of hardware that support the AN functionality: Mellanox 4 (MLX4) and Mellanox 5 (MLX5). ASA Virtual supports AN for Mellanox hardware for the following instances from Release 9.15:

- D3, D3_v2, DS3, DS3_v2
- D4, D4_v2, DS4, DS4_v2
- D5, D5_v2, DS5, DS5_v2
- D8_v3, D8s_v3
- D16_v3, D16s_v3
- F4, F4s
- F8, F8s, F8s_v2
- F16, F16s, F16s_v2

Note MLX4 (Mellanox 4) is also referred to as connectx3 = cx3, and MLX5 (Mellanox 5) is also referred as connectx4 = cx4.

You cannot specify which NIC Azure uses MLX4 or MLX5 for your VM deployment. Cisco recommends that you upgrade to ASA Virtual 9.15 version or later to use the accelerated networking functionality.

Support for MANA NIC Hardware

ASA Virtual supports MANA NIC hardware on Microsoft Azure for the following instances from Release 9.24:

- Standard_D8s_v5
- Standard_D16s_v5

Note To maintain optimal performance and prevent automatic transitions to a synthetic path for stop-deallocated and restarted or redeployed VMs, ensure that all VMs on version 10.0.0 and earlier opt out of MANA NIC eligibility. For more information, refer to MANA support for NVAs.

Deploy the ASA Virtual

You can deploy the ASA Virtual on Microsoft Azure.

- Deploy the ASA Virtual as a stand-alone firewall using the Azure Resource Manager on the standard Azure public cloud and the Azure Government environments. See Deploy the ASAv from Azure Resource Manager.
- Deploy the ASA Virtual as an integrated partner solution within Azure using the Azure Security Center. Security-conscious customers are offered the ASA Virtual 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.
- Deploy an ASA Virtual High Availablity pair using the Azure Resource Manager. To ensure redundancy, you can deploy the ASA Virtual in an Active/Backup high availability (HA) configuration. HA in the public cloud implements a stateless Active/Backup solution that allows for a failure of the active ASA Virtual to trigger an automatic failover of the system to the backup ASA Virtual. See Deploy the ASA Virtual for High Availability from Azure Resource Manager, on page 18.
- Deploy the ASA Virtual or an ASA Virtual High Availablity pair with a custom template using a Managed Image from a VHD (available from cisco.com). Cisco provides a compressed virtual hard disk (VHD) that you can upload to Azure to simplify the process of deploying the ASA Virtual. Using a Managed Image and two JSON files (a Template file and a Parameter File), you can deploy and provision all the resources for the ASA Virtual in a single, coordinated operation. To use the custom template, see Deploy the ASA Virtual from Azure Using a VHD and Resource Template, on page 19.

Note While searching for Cisco offers in Marketplace, you may find two different offers with similar names, but different offer types, Application Offer and Virtual Machine Offer.

For marketplace deployments, use ONLY the Application Offers.

Virtual Machine offer (may be visible) with VMSR (Virtual Machine Software Reservations) plan in marketplace. These are specific Multiparty Private Offer plans specifically for channel/resale and should be ignored for regular deployments.

Application Offers available in Marketplace:

- Cisco Secure Firewall ASA Virtual - BYOL and PAYG
- Cisco Secure Firewall ASA Virtual - High Availability Pair - BYOL

Deploy the ASA Virtual from Azure Resource Manager

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

When you deploy the ASA Virtual 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

Step 1 Log into the Azure Resource Manager (ARM) portal.

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

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

Step 3 Configure the basic settings.

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

Important
If your name is not unique and you reuse an existing name, the deployment will fail.

b) Enter your username.

c) Choose an authentication type, either **Password** or **SSH public key**.

If you choose **Password**, enter a password and confirm. See Password Setup for guidelines on password complexity.

d) If you are using the ASAv you are deploying as a cluster, then create and enter the basic day0 configuration details in the **ASAv Day0 configuration (user-data)** field.

For information on creating day0 configuration for ASAv in Azure, see Configure the ASA Virtual Clustering Using a Day0 Configuration in the Deploy a Cluster for the ASA Virtual for the Private Cloud guide.

e) Choose your subscription type.

f) Choose a **Resource group**.

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

g) Choose your location.

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

h) Click **OK**.

Step 4 Configure the ASA Virtual settings.

a) Choose the virtual machine size.

b) Choose a storage account.

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**.

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.

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 ASA Virtual will deploy to, and then click **OK**.

Important
Each interface must be attached to a unique subnet.

g) Click **OK**.

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

Step 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 for instructions for accessing the ASDM.

Deploy the ASA Virtual 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 ASA Virtual as a firewall solution to Azure customers.

As an integrated solution in Security Center, you can rapidly deploy the ASA Virtual 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 ASA Virtual from Security Center. For more detailed information, see Azure Security Center.

Procedure

Step 1 Log into the Azure portal.

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

Step 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.

Step 3 On the **Security Center** blade, choose the **Policy** tile.

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

Step 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 ASA Virtual is a recommended solution in Security Center.
b) Set any other recommendations as needed.

Step 6 Return to the **Security Center** blade and 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.

Step 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.

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

Step 9 Configure the basic settings.

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

Important
If your name is not unique and you reuse an existing name, 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. See Password Setup for guidelines on password complexity.

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**.

Step 10 Configure the ASA Virtual settings.

a) Choose the virtual machine size.

The ASA Virtual supports Standard D3 and Standard D3_v2.

b) Choose a storage account.

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**.

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.

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 ASA Virtual will deploy to, and then click **OK**.

Important
Each interface must be attached to a unique subnet.

g) Click **OK**.

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

Step 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 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 the ASA Virtual for High Availability from Azure Resource Manager

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

ASA Virtual HA in Azure deploys two ASA Virtuals 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

Step 1 Log into the Azure portal.

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

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

Step 3 Configure the **Basics** settings.

a) Enter a prefix for the ASA Virtual machine names. The ASA Virtual names will be ‘prefix’-A and ‘prefix’-B.

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

b) Enter a **Username**.

This will be the administrative username for both Virtual Machines.

Important
The username **admin** is not allowed in Azure.

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

If you choose **Password**, enter a password and confirm. See Password Setup for guidelines on password complexity.

d) Choose your subscription type.

e) 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.

f) Choose your **Location**.

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

g) Click **OK**.

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

a) Choose the Virtual Machine size.

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

Important
ASA HA mode always uses **Managed**.

Step 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.

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.

Step 6 Repeat the previous steps for the **ASAv-B** settings.

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

a) Configure the four subnets that the ASA Virtual will deploy to, and then click **OK**.

Important
Each interface must be attached to a unique subnet.

b) Click **OK**.

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

Step 9 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 for instructions for accessing the ASDM.
- See the 'Failover for High Availability in the Public Cloud' chapter in the ASA Series General Operations Configuration Guide for more information about ASA Virtual HA configuration in Azure.

Deploy the ASA Virtual from Azure Using a VHD and Resource Template

You can create your own custom ASA Virtual images using a compressed VHD image available from Cisco. To deploy using a VHD image, you must upload the VHD image to your Azure storage account. Then, you

can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.

Before you begin

- You need the JSON template and corresponding JSON parameter file for your ASA Virtual template deployment. You can download template files from the GitHub repository at:

  https://github.com/CiscoDevNet/cisco-asav/tree/master/deployment-templates/azure

- For instructions on how to build a template and a parameter file, see Appendix — Azure Resource Template Example, on page 34.
- This procedure requires an existing Linux VM in Azure. We recommended you use a temporary Linux VM (such as Ubuntu 16.04) to upload the compressed VHD image to Azure. This image will require about 50G of storage when unzipped. Also, your upload times to Azure storage will be faster from a Linux VM in Azure.

  If you need to create a VM, use one of the following methods:

  - Create a Linux virtual machine with the Azure CLI
  - Create a Linux virtual machine in the Azure portal

- In your Azure subscription, you should have a storage account available in the Location in which you want to deploy the ASA Virtual.

Procedure

Step 1 Download the ASA Virtual compressed VHD image from the https://software.cisco.com/download/home page:

a) Navigate to **Products** > **Security** > **Firewalls** > **Adaptive Security Appliances (ASA)** > **Adaptive Security Appliance (ASA) Software**.

b) Click **Adaptive Security Virtual Appliance (ASAv)**.

Follow the instructions for downloading the image.

For example, asav9-14-1.vhd.bz2

Step 2 Copy the compressed VHD image to your Linux VM in Azure.

There are many options that you can use to move files up to Azure and down from Azure. This example shows SCP or secure copy:

```
# scp /username@remotehost.com/dir/asav9-14-1.vhd.bz2 <linux-ip>
```

Step 3 Log in to the Linux VM in Azure and navigate to the directory where you copied the compressed VHD image.

Step 4 Unzip the ASA Virtual VHD image.

There are many options that you can use to unzip or decompress files. This example shows the Bzip2 utility, but there are also Windows-based utilities that would work.

```
# bunzip2 asav9-14-1.vhd.bz2
```

Step 5 Upload the VHD to a container in your Azure storage account. You can use an existing storage account or create a new one. The storage account name can only contain lowercase letters and numbers.

There are many options that you can use to upload a VHD to your storage account, including AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI, or the Azure Portal. We do not recommend using the Azure Portal for a file as large as the ASA Virtual.

The following example shows the syntax using Azure CLI:

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

Step 6 Create a Managed Image from the VHD:

a) In the Azure Portal, select **Images**.
b) Click **Add** to create a new image.
c) Provide the following information:

- **Subscription**—Choose a subscription from the drop-down list.
- **Resource group**—Choose an existing resource group or create a new one.
- **Name**—Enter a user-defined name for the managed image.
- **Region**—Choose the region in which the VM Is deployed.
- **OS type**—Choose **Linux** as the OS type.
- **VM generation**

  Choose **Generation 1** for BIOS boot mode.

  Choose **Generation 2** for UEFI boot mode.
- **Storage blob**—Browse to the storage account to select the uploaded VHD.
- **Account type**—As per your requirement, choose Standard HDD, Standard SSD, or Premium SSD, from the drop-down list.

  When you select the VM size planned for deployment of this image, ensure that the VM size supports the selected account type.
- **Host caching**—Choose Read/write from the drop-down list.
- **Data disks**—Leave at default; don't add a data disk.

d) Click **Create**.

Wait for the **Successfully created image** message under the **Notifications** tab.

Note
Once the Managed Image has been created, the uploaded VHD and upload Storage Account can be removed.

Step 7 Acquire the Resource ID of the newly created Managed Image.

Internally, Azure associates every resource with a Resource ID. You'll need the Resource ID when you deploy new ASA Virtual firewalls from this managed image.

a) In the Azure Portal, select **Images**.

b) Select the managed image created in the previous step.
c) Click **Overview** to view the image properties.
d) Copy the **Resource ID** to the clipboard.

The **Resource ID** takes the form of:

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>
/providers/Microsoft.Compute/<container>/ <vhdname>

Step 8 Build an ASA Virtual firewall using the managed image and a resource template:

a) Select **New**, and search for **Template Deployment** until you can select it from the options.
b) Select **Create**.
c) Select **Build your own template in the editor**.

You have a blank template that is available for customizing. See Create a Resource Template, on page 36 for an example of how to create a template

d) Paste your customized JSON template code into the window, and then click **Save**.
e) Choose a **Subscription** from the drop-down list.
f) Choose an existing **Resource group** or create a new one.
g) Choose a **Location** from the drop-down list.
h) Paste the Managed Image **Resource ID** from the previous step into the **Vm Managed Image Id** field.

Step 9 Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.

a) Click **Load file** and browse to the customized ASA Virtual parameter file. See Create a Parameter File, on page 44 for an example of how to create a parameter template.
b) Paste your customized JSON parameters code into the window, and then click **Save**.

Step 10 Review the Custom deployment details. Make sure that the information in **Basics** and **Settings** matches your expected deployment configuration, including the **Resource ID**.

Step 11 Review the Terms and Conditions, and check the **I agree to the terms and conditions stated above** check box.

Step 12 Click **Purchase** to deploy an ASA Virtual firewall using the managed image and a custom template.

If there are no conflicts in your template and parameter files, you should have a successful deployment.

The Managed Image is available for multiple deployments within the same subscription and region.

What to do next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page87 for instructions for accessing the ASDM.

Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment

This applies only for the Azure Private Marketplace users. If you are using Azure Private Marketplace, then ensure that both Application Offers and required Virtual Machine Offers (hidden) are enabled for the user in respective private marketplace.

Virtual Machine Offers and Plans (hidden):

- Publisher ID: **cisco**
- Cisco Secure Firewall ASA Virtual VM Offers (used for both the Cisco Secure Firewall ASA Virtual Application offers)
  - Offer ID: **cisco-asav**
  - BYOL Plan ID: **asav-azure-byol**
  - PAYG Plan ID: **asav-azure-payg**

When user deploys the visible application offer from Marketplace, based on user selection of PAYG or BYOL licensing corresponding image from the VM offer plan is referenced and deployed.

Therefore, for the deployment to work, both Application and VM offers needs to be enabled/available on the Private Marketplace for the Azure tenant/subscription.

Refer the Azure documentation for enabling these application and VM offers in private marketplaces.

- Govern and control using private Azure Marketplace
- Add an offer to a private marketplace
- Set-AzMarketplacePrivateStoreOffer

Application offers are easily enabled via Azure UI as they are visible in the marketplace.

In order to enable hidden virtual machine offers in private marketplace, you might have to rely on CLI commands (at the time of this doc creation only CLI way is possible).

Sample command:

Cisco Secure Firewall ASA Virtual BYOL plan can be enabled using similar sample command given below:

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-asav'
  SpecificPlanIdsLimitation =@('asav-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

Note The sample command is only for reference, check Azure documentation for more details.

Reference Error message

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
```

```
     "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be purchased
 due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's Private
 Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors for
details. "
}
```

User may run into the above error while deploying the Marketplace offer. To resolve this, both Application and VM offers need to be enabled/available on the Azure tenant/subscription.

Deploy the IPv6 Supported ASA Virtual on Azure

This chapter explains how to deploy the IPv6 Supported ASA Virtual from the Azure portal.

About IPv6 Supported Deployment on Azure

ASA Virtual offerings support both IPV4 and IPv6 from 9.19 and later. In Azure, you can deploy ASA Virtual directly from the Marketplace offering, which creates or uses a virtual network, but currently, a limitation in Azure restricts the Marketplace application offer to use or create only IPv4-based VNet/subnets. Although, you can manually configure the IPv6 addresses to the existing VNet, a new ASA Virtual instance cannot be added to the VNet configured with the IPv6 subnets. Azure imposes certain restrictions to deploy any third-party resources using an alternative approach other than deploying resources through Marketplace.

Cisco is currently offering two methods to deploy ASA Virtual to support IPv6 addressing.

The following two distinct custom IPv6 templates are offered, where:

- **Custom IPv6 template (ARM template)** — It is offered to deploy ASA Virtual with IPv6 configuration using an Azure Resource Manager (ARM) template that internally refers to a marketplace image on Azure. This template contains JSON files with resources and parameter definitions that you can configure to deploy IPv6-supported ASA Virtual. To use this template, see Deploy from Azure Using Custom IPv6 Template with Marketplace Image Reference, on page 25.

  Programmatic deployment is a process of granting access to the VM images on Azure Marketplace to deploy custom templates through PowerShell, Azure CLI, ARM template, or API. You are restricted to deploy these custom templates on VM without providing access to VMs. If you attempt to deploy such custom templates on VM, then the following error message is displayed:

  Legal terms have not been accepted for this item on this subscription. To accept legal terms ….and configure programmatic deployment for the Marketplace item …..

  You can use one of the following methods to enable Programmatic deployment in Azure to deploy the custom IPv6 (ARM) template refering to the marketplace image:

  - **Azure Portal** – Enable programmatic deployment option corresponding to the ASA Virtual offering available on Azure Marketplace for deploying the custom IPv6 template (ARM template).

- **Azure CLI** – Run the CLI command to enable programmatic deployment for deploying the custom IPv6 (ARM template).

- **Custom VHD image and IPv6 template (ARM template)** — Create a managed image using the VHD image and ARM template on Azure. This process is similar to deploying ASA Virtual by using a VHD and resource template. This template refers to a managed image during deployment and uses an ARM template which you can upload and configure on Azure to deploy IPv6-supported ASA Virtual. See, Deploy from Azure Using a VHD and Custom IPv6 Template, on page 30.

The process involved in deploying ASA Virtual using custom IPv6 template (ARM template) in reference to marketplace image or VHD image with custom IPv6 template.

The steps involved in deploying the ASA Virtual is as follows:

Table 3:

Step	Process
1	Create a Linux VM in Azure where you are planning to deploy the IPv6-supported ASA Virtual
2	Enable Programmatic deployment option on Azure portal or Azure CLI **only** when you are deploying ASA Virtual using the custom IPv6 template with Marketplace image reference.
3	Depending on the type of deployment download the following custom templates: • Custom IPv6 Template with Azure Marketplace reference image. VHD image with custom IPv6 (ARM) template.
4	Update the IPv6 parameters in the custom IPv6 (ARM) template. **Note** The equivalent Software image version parameter value of the marketplace image version is required only when you are deploying ASA Virtual using the custom IPv6 template with Marketplace image reference. You must run a command to retrieve the Software version details.
5	Deploy the ARM template through Azure portal or Azure CLI.

Deploy from Azure Using Custom IPv6 Template with Marketplace Image Reference

The process involved in deploying ASA Virtual using custom IPv6 template (ARM template) in reference to marketplace image.

Procedure

Step 1 Log into the Azure portal.

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

Step 2 Enable Programmatic deployment through Azure portal or Azure CLI as follows:

To enable this option on Azure Portal.

a) Under **Azure Services**, click **Subscriptions** to view the subscription blade page.
b) On the left pane, click **Programmatic Deployment** under the **Settings** option.

All the types of resources deployed on the VM are displayed along with the associated subscription offerings.

c) Click **Enable** under the **Status** column and corresponding to the ASA Virtual offering to obtain for programmatic deployment of the custom IPv6 template.

OR

To enable this option through Azure CLI.

a) Go to the Linux VM.
b) Run the following CLI command to enable programmatic deployment for deploying custom IPv6 (ARM) template.

During the command execution, you must only accept the terms once per subscription of the image.

 # Accept terms

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # Review that terms were accepted (i.e., accepted=true)

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

Where,

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-asav'
- **<sku/plan>** - 'asav-azure-byol'

The following is a command script example to enable programmatic deployment for deploying ASA Virtual with BYOL subscription plan.

- **az vm image terms show -p cisco -f cisco-ftdv --plan asav-azure-byol**

Step 3 Run the following command to retrieve the Software version details equivalent to the marketplace image version.

az vm image list --all -p <publisher> -f <offer> -s <sku>

Where,

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-asav'
- **<sku>** - 'asav-azure-byol'

The following is a command script example to retrieve the Software version details equivalent to the marketplace image version for ASA Virtual.

az vm image list --all -p cisco -f cisco-ftdv -s asav-azure-byol

Step 4 Select one of the ASA Virtual version from the list of available marketplace image versions that are displayed.

For IPv6 support deployment of ASA Virtual, you must select the ASA Virtual version as 919*or higher.

Step 5 Download the marketplace custom IPv6 template (ARM templates) from the Cisco GitHub repository.

Step 6 Prepare the parameters file by providing the deployment values in the parameters template file (JSON).

The following table describes the deployment values you need to enter in the custom IPv6 template parameters for ASA Virtual custom deployment:

Parameter Name	Examples of allowed Values/Type	Description
vmName	cisco-asav	Name the ASA Virtual VM in Azure.
softwareVersion	919.0.24	The software version of the marketplace image version.
adminUsername	hjohn	The username to log into ASA Virtual. You cannot use the reserved name 'admin', which is assigned to administrator.
adminPassword	E28@4OiUrhx!	The admin password. Password combination must be an alphanumeric characters with 12 to 72 characters long. The password combination must comprise of lowercase and uppercase letters, numbers and special characters. See Password Setup for guidelines on password complexity.
vmStorageAccount	hjohnvmsa	Your Azure storage account. You can use an existing storage account or create a new one. The storage account characters must be between three and 24 characters long. The password combination must contain only lowercase letters and numbers.
availabilityZone	0	Specify the availability zone for deployment, public IP and the virtual machine will be created in the specified availability zone. Set it to '**0**' if you do not need availability zone configuration. Ensure that selected region supports availability zones and value provided is correct. (This must be an integer between 0-3).
userData	`!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6`	User Data passed down to the Virtual Machine.

Parameter Name	Examples of allowed Values/Type	Description
	`enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0 management\nssh timeout 60\nssh version 2\nusername admin password E28@4OiUrhx! privilege 15\nenable password E28@4OiUrhx!\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain-lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	
virtualNetworkResourceGroup	cisco-asav-rg	Name of the resource group containing the virtual network. In case virtualNetworkNewOr Existing is new, this value should be same as resource group selected for template deployment.
virtualNetworkName	cisco-asav-vnet	The name of the virtual network.
virtualNetworkNewOrExisting	new	This parameter determines whether a new virtual network should be created or an existing virtual network is to be used.
virtualNetworkAddressPrefixes	10.151.0.0/16	IPv4 address prefix for the virtual network, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	IPv6 address prefix for the virtual network, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet1Name	mgmt	Management subnet name.
Subnet1Prefix	10.151.1.0/24	Management subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	Management subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.

Parameter Name	Examples of allowed Values/Type	Description
subnet1StartAddress	10.151.1.4	Management interface IPv4 address.
subnet1v6StartAddress	ace:cab:deca:1111::6	Management interface IPv6 address.
Subnet2Name	diag	Data interface 1 subnet name.
Subnet2Prefix	10.151.2.0/24	Data interface 1 Subnet IPv4 prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	Data interface 1 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet2StartAddress	10.151.2.4	Data interface 1 IPv4 address.
subnet2v6StartAddress	ace:cab:deca:2222::6	Data interface 1 IPv6 address.
Subnet3Name	inside	Data interface 2 subnet name.
Subnet3Prefix	10.151.3.0/24	Data interface 2 Subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	Data interface 2 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet3StartAddress	10.151.3.4	Data interface 2 IPv4 address.
subnet3v6StartAddress	ace:cab:deca:3333::6	Data interface 2 IPv6 address.
Subnet4Name	outside	Data interface 3 subnet name.
Subnet4Prefix	10.151.4.0/24	Data interface 3 subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	Data interface 3 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet4StartAddress	10.151.4.4	Data interface 3 IPv4 Address.
subnet4v6StartAddress	ace:cab:deca:4444::6	Data interface 3 IPv6 Address.

Parameter Name	Examples of allowed Values/Type	Description
vmSize	Standard_D4_v2	Size of the ASA Virtual VM. Standard_D3_v2 is the default.

Step 7 Use the ARM template to deploy ASA Virtual firewall through the Azure portal or Azure CLI. For information about deploying the ARM template on Azure, refer to the following Azure documentation:

- Create and deploy ARM templates by using the Azure portal
- Deploy a local ARM template through CLI

What to do next

Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM 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 from Azure Using a VHD and Custom IPv6 Template

You can create your own custom ASA Virtual images using a compressed VHD image available from Cisco. This process is similar to deploying ASA Virtual by using a VHD and resource template.

Before you begin

- You need the JSON template and corresponding JSON parameter file for your ASA Virtual deployment using VHD and ARM updated template on Github, where you'll find instructions on how to build a template and parameter file.
- This procedure requires an existing Linux VM in Azure. We recommended you use a temporary Linux VM (such as Ubuntu 16.04) to upload the compressed VHD image to Azure. This image will require about 50GB of storage when unzipped. Also, your upload times to Azure storage will be faster from a Linux VM in Azure.

  If you need to create a VM, use one of the following methods:

  - Create a Linux virtual machine with the Azure CLI
  - Create a Linux virtual machine with the Azure portal
- In your Azure subscription, you should have a storage account available in the Location in which you want to deploy the ASA Virtual.

Procedure

Step 1 Download the ASA Virtual compressed VHD image (*.bz2) from the Cisco Download Software page:

a) Navigate to **Products** > **Security** > **Firewalls** > **Adaptive Security Appliances (ASA)** > **Adaptive Security Appliance (ASA) Software**.

b) Click **Adaptive Security Virtual Appliance (ASAv)**.

Follow the instructions for downloading the image.

For example, asav9-14-1.vhd.bz2

Step 2 Perform **Step 2** through **Step 8** in Deploy the ASA Virtual from Azure Using a VHD and Resource Template.

Step 3 Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.

a) Click **Load** file and browse to the customized ASA Virtual parameter file. See the sample for the Azure ASA Virtual deployment using VHD and custom IPv6 (ARM) template on Github, where you'll find instructions on how to build a template and parameter file.

b) Paste your customized JSON parameters code into the window, and then click **Save**.

The following table describes the deployment values you need to enter in the custom IPv6 template parameters for ASA Virtual deployment:

Parameter Name	Examples of allowed values/types	Description
vmName	cisco-asav	Name the ASA Virtual VM in Azure.
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	The ID of the image used for deployment. Internally, Azure associates every resource with a Resource ID.
adminUsername	hjohn	The username to log into ASA Virtual. You cannot use the reserved name 'admin', which is assigned to administrator.
adminPassword	E28@4OiUrhx!	The admin password. Password combination must be an alphanumeric characters with 12 to 72 characters long. The password combination must comprise of lowercase and uppercase letters, numbers and special characters.
vmStorageAccount	hjohnvmsa	Your Azure storage account. You can use an existing storage account or create a new one. The storage account characters must be between three and 24 characters long. The password combination must contain only lowercase letters and numbers.
availabilityZone	0	Specify the availability zone for deployment, public IP and the virtual machine will be created in the specified availability zone.

Parameter Name	Examples of allowed values/types	Description
		Set it to '**0**' if you do not need availability zone configuration. Ensure that selected region supports availability zones and value provided is correct. (This must be an integer between 0-3).
userData	`!\ninterface management0\/0\nmanagement-only\nnameif management\nsecurity-level 100\nip address dhcp setroute\nipv6 enable\nipv6 address dhcp\nno shutdown\n!\ncrypto key generate rsa modulus 2048\nssh 0 0 management\nssh timeout 60\nssh version 2\nusername admin password E28@4OiUrhx! privilege 15\nenable password E28@4OiUrhx!\nusername admin attributes\nservice-type admin\naaa authentication ssh console LOCAL\n!\naccess-list allow-all extended permit ip any any\naccess-group allow-all global\n!\ndns domain -lookup management\ndns server-group DefaultDNS\nname-server 8.8.8.8\n!`	User Data passed down to the Virtual Machine.
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	The field to provide in the Day 0 configuration to the ASA Virtual. By default it has the following three key-value pairs to configure: • 'admin' user password • CSF-MCv hostname • the CSF-MCv hostname or CSF-DM for management. 'ManageLocally : yes' - This configures the CSF-DM to be used as Firewall Threat Defense Virtual manager. You can configure the CSF-MCv as Firewall Threat Defense Virtual manager and also give the inputs for fields required to configure the same on CSF-MCv.
virtualNetworkResourceGroup	cisco-asav	Name of the resource group containing the virtual network. In case virtualNetworkNewOr Existing is new, this value should be same as resource group selected for template deployment.

Parameter Name	Examples of allowed values/types	Description
virtualNetworkName	cisco-asav-vnet	The name of the virtual network.
virtualNetworkNewOrExisting	new	This parameter determines whether a new virtual network should be created or an existing virtual network is to be used.
virtualNetworkAddressPrefixes	10.151.0.0/16	IPv4 address prefix for the virtual network, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	IPv6 address prefix for the virtual network, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet1Name	mgmt-ipv6	Management subnet name.
Subnet1Prefix	10.151.1.0/24	Management subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	Management subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet1StartAddress	10.151.1.4	Management interface IPv4 address.
subnet1v6StartAddress	ace:cab:deca:1111::6	Management interface IPv6 address.
Subnet2Name	diag	Data interface 1 subnet name.
Subnet2Prefix	10.151.2.0/24	Data interface 1 Subnet IPv4 prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	Data interface 1 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet2StartAddress	10.151.2.4	Data interface 1 IPv4 address.
subnet2v6StartAddress	ace:cab:deca:2222::6	Data interface 1 IPv6 address.
Subnet3Name	inside	Data interface 2 subnet name.
Subnet3Prefix	10.151.3.0/24	Data interface 2 Subnet IPv4 Prefix, this is required only if

Parameter Name	Examples of allowed values/types	Description
		'virtualNetworkNewOr Existing' is set to 'new'.
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	Data interface 2 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet3StartAddress	10.151.3.4	Data interface 2 IPv4 address.
subnet3v6StartAddress	ace:cab:deca:3333::6	Data interface 2 IPv6 address.
Subnet4Name	outside	Data interface 3 subnet name.
Subnet4Prefix	10.151.4.0/24	Data interface 3 subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	Data interface 3 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet4StartAddress	10.151.4.4	Data interface 3 IPv4 Address.
subnet4v6StartAddress	ace:cab:deca:4444::6	Data interface 3 IPv6 Address.
vmSize	Standard_D4_v2	Size of the ASA Virtual VM. Standard_D3_v2 is the default.

Step 4 Use the ARM template to deploy ASA Virtual firewall through the Azure portal or Azure CLI. For information about deploying the ARM template on Azure, refer to the following Azure documentation:

- Create and deploy ARM templates by using the Azure portal
- Deploy a local ARM template through CLI

What to do next

- Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM, page87 for instructions for accessing the ASDM.

Appendix — Azure Resource Template Example

This section describes the structure of an Azure Resource Manager template you can use to deploy the ASA Virtual. An Azure Resource Template is a JSON file. To simplify the deployment of all the required resources, this example includes two JSON files:

- **Template File**—This is the main resources file that deploys all the components within the resource group.
- **Parameter File**—This file includes the parameters required to successfully deploy the ASA Virtual. It includes details such as the subnet information, virtual machine tier and size, username and password for the ASA Virtual, the name of the storage container, etc. You can customize this file for your Azure Stack Hub deployment environment.

Template File Format

This section describes the structure of an Azure Resource Manager template file. The following example shows a collapsed view of a template file and presents the different sections of a template.

Azure Resource Manager JSON Template File

```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "",
    "parameters": { },
    "variables": { },
    "resources": [ ],
    "outputs": { }
}
```

The template consists of JSON and expressions that you can use to construct values for your ASA Virtual deployment. In its simplest structure, a template contains the following elements:

Table 4: Azure Resource Manager JSON Template File Elements Defined

Element	Required	Description
$schema	Yes	Location of the JSON schema file that describes the version of the template language. Use the URL shown in the preceding figure.
contentVersion	Yes	Version of the template (such as 1.0.0.0). You can provide any value for this element. When deploying resources using the template, this value can be used to make sure that the right template is being used.
parameters	No	Values that are provided when deployment is executed to customize resource deployment. Parameters allow for inputting values at the time of deployment. They are not absolutely required, but without them the JSON template will deploy the resources with the same parameters each time.
variables	No	Values that are used as JSON fragments in the template to simplify template language expressions.
resources	Yes	Resource types that are deployed or updated in a resource group.
outputs	No	Values that are returned after deployment.

You can make use of JSON templates to not only declare the resource types to be deployed, but also their related configuration parameters. The following example shows a template that deploys a new ASA Virtual.

Create a Resource Template

You can use the example below to create your own deployment template using a text editor.

Procedure

Step 1 Copy the text in the following example.

Example:

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "vmName": {
            "type": "string",
            "defaultValue": "ngfw",
            "metadata": {
                "description": "Name of the NGFW VM"
            }
        },
        "vmManagedImageId": {
            "type": "string",
            "defaultValue":
"/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage",

            "metadata": {
                "description": "The ID of the managed image used for deployment.
/subscriptions/{subscription-id}/resourceGroups/myresourcegroup1/providers/Microsoft.Compute/images/myImage"

            }
        },
        "adminUsername": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "Username for the Virtual Machine. admin, Administrator among other
values are disallowed - see Azure docs"
            }
        },
        "adminPassword": {
            "type": "securestring",
            "defaultValue" : "",
            "metadata": {
                "description": "Password for the Virtual Machine. Passwords must be 12 to 72 chars
and have at least 3 of the following: Lowercase, uppercase, numbers, special chars"
            }
        },
        "vmStorageAccount": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
               "description": "A storage account name (boot diags require a storage account). Between
 3 and 24 characters. Lowercase letters and numbers only"
            }
```

```
},
"virtualNetworkResourceGroup": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "Name of the virtual network's Resource Group"
    }
},
"virtualNetworkName": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "Name of the virtual network"
    }
},
"mgmtSubnetName": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "The FTDv management interface will attach to this subnet"
    }
},
"mgmtSubnetIP": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "NGFW IP on the mgmt interface (example: 192.168.0.10)"
    }
},
"diagSubnetName": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "The FTDv diagnostic0/0 interface will attach to this subnet"
    }
},
"diagSubnetIP": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "NGFW IP on the diag interface (example: 192.168.1.10)"
    }
},
"gig00SubnetName": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "The FTDv Gigabit 0/0 interface will attach to this subnet"
    }
},
"gig00SubnetIP": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "The IP on the Gigabit 0/0 interface (example: 192.168.2.10)"
    }
},
"gig01SubnetName": {
    "type": "string",
    "defaultValue": "",
    "metadata": {
        "description": "The FTDv Gigabit 0/1 interface will attach to this subnet"
    }
},
```

```
            "gig01SubnetIP": {
                "type": "string",
                "defaultValue": "",
                "metadata": {
                    "description": "The IP on the Gigabit 0/1 interface (example: 192.168.3.5)"
                }
            },
            "VmSize": {
                "type": "string",
                "defaultValue": "Standard_D3_v2",
                "allowedValues": [ "Standard_D3_v2" , "Standard_D3" ],
                "metadata": {
                    "description": "NGFW VM Size (Standard_D3_v2 or Standard_D3)"
                }
            }
        },
        "variables": {

            "virtualNetworkID":
"[resourceId(parameters('virtualNetworkResourceGroup'),'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",

            "vmNic0Name":"[concat(parameters('vmName'),'-nic0')]",
            "vmNic1Name":"[concat(parameters('vmName'),'-nic1')]",
            "vmNic2Name":"[concat(parameters('vmName'),'-nic2')]",
            "vmNic3Name":"[concat(parameters('vmName'),'-nic3')]",

            "vmNic0NsgName":"[concat(variables('vmNic0Name'),'-NSG')]",

            "vmMgmtPublicIPAddressName": "[concat(parameters('vmName'),'nic0-ip')]",
            "vmMgmtPublicIPAddressType": "Static",
            "vmMgmtPublicIPAddressDnsName": "[variables('vmMgmtPublicIPAddressName')]"
        },
        "resources": [
            {
                "apiVersion": "2017-03-01",
                "type": "Microsoft.Network/publicIPAddresses",
                "name": "[variables('vmMgmtPublicIPAddressName')]",
                "location": "[resourceGroup().location]",
                "properties": {
                  "publicIPAllocationMethod": "[variables('vmMgmtPublicIpAddressType')]",
                  "dnsSettings": {
                    "domainNameLabel": "[variables('vmMgmtPublicIPAddressDnsName')]"
                  }
                }
            },
            {
                "apiVersion": "2015-06-15",
                "type": "Microsoft.Network/networkSecurityGroups",
                "name": "[variables('vmNic0NsgName')]",
                "location": "[resourceGroup().location]",
                "properties": {
                    "securityRules": [
                        {
                            "name": "SSH-Rule",
                            "properties": {
                                "description": "Allow SSH",
                                "protocol": "Tcp",
                                "sourcePortRange": "*",
                                "destinationPortRange": "22",
                                "sourceAddressPrefix": "Internet",
                                "destinationAddressPrefix": "*",
                                "access": "Allow",
                                "priority": 100,
```

```
                            "direction": "Inbound"
                        }
                    },
                    {
                        "name": "SFtunnel-Rule",
                        "properties": {
                            "description": "Allow tcp 8305",
                            "protocol": "Tcp",
                            "sourcePortRange": "*",
                            "destinationPortRange": "8305",
                            "sourceAddressPrefix": "Internet",
                            "destinationAddressPrefix": "*",
                            "access": "Allow",
                            "priority": 101,
                            "direction": "Inbound"
                        }
                    }
                ]
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic0Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkSecurityGroups/',variables('vmNic0NsgName'))]",
                "[concat('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('mgmtSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('mgmtSubnetName'))]"
                            },
                            "publicIPAddress":{
                                "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('vmMgmtPublicIPAddressName'))]"
                            }
                        }
                    }
                ],
                "networkSecurityGroup": {
                    "id": "[resourceId('Microsoft.Network/networkSecurityGroups',
variables('vmNic0NsgName'))]"
                },
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic1Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
```

```
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('diagSubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('diagSubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic2Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig00SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig00SubnetName'))]"
                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "apiVersion": "2017-03-01",
            "type": "Microsoft.Network/networkInterfaces",
            "name": "[variables('vmNic3Name')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
            ],
            "properties": {
                "ipConfigurations": [
                    {
                        "name": "ipconfig1",
                        "properties": {
                            "privateIPAllocationMethod": "Static",
                            "privateIPAddress" : "[parameters('gig01SubnetIP')]",
                            "subnet": {
                                "id": "[concat(variables('virtualNetworkID'),'/subnets/',
parameters('gig01SubnetName'))]"

                            }                        }
                    }
                ],
                "enableIPForwarding": true
            }
        },
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[concat(parameters('vmStorageAccount'))]",
```

```
            "apiVersion": "2015-06-15",
            "location": "[resourceGroup().location]",
            "properties": {
              "accountType": "Standard_LRS"
            }
        },
        {
            "apiVersion": "2017-12-01",
            "type": "Microsoft.Compute/virtualMachines",
            "name": "[parameters('vmName')]",
            "location": "[resourceGroup().location]",
            "dependsOn": [
                "[concat('Microsoft.Storage/storageAccounts/', parameters('vmStorageAccount'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic0Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic1Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic2Name'))]",
                "[concat('Microsoft.Network/networkInterfaces/',variables('vmNic3Name'))]"
            ],
            "properties": {
                "hardwareProfile": {
                    "vmSize": "[parameters('vmSize')]"
                },
                "osProfile": {
                    "computername": "[parameters('vmName')]",
                    "adminUsername": "[parameters('AdminUsername')]",
                    "adminPassword": "[parameters('AdminPassword')]"
                },
                "storageProfile": {
                    "imageReference": {
                        "id": "[parameters('vmManagedImageId')]"
                    },
                    "osDisk": {
                        "osType": "Linux",
                        "caching": "ReadWrite",
                        "createOption": "FromImage"
                    }
                },
                "networkProfile": {
                    "networkInterfaces": [
                        {
                            "properties": {
                                "primary": true
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic0Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic1Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic2Name'))]"
                        },
                        {
                            "properties": {
                                "primary": false
                            },
```

```
                            "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('vmNic3Name'))]"
                            }
                        ]
                    },
                    "diagnosticsProfile": {
                        "bootDiagnostics": {
                            "enabled": true,
                            "storageUri":
"[concat('http://',parameters('vmStorageAccount'),'.blob.core.windows.net')]"
                        }
                    }
                }
            }
        ],
        "outputs": {  }
}
```

Step 2 Save the file locally as a JSON file; for example, **azureDeploy.json**.

Step 3 Edit the file to create a template to suit your deployment parameters.

Step 4 Use this template to deploy the ASA Virtual as described in Deploy the ASA Virtual from Azure Using a VHD and Resource Template, on page 19.

Parameter File Format

When you start a new deployment, you have parameters defined in your resource template. These need to be entered before the deployment can start. You can manually enter the parameters that you have defined in your resource template, or you can put the parameters in a template parameters JSON file.

The parameter file contains a value for each parameter shown in the parameters example in Create a Parameter File, on page 44. These values are automatically passed to the template during deployment. You can create multiple parameter files for different deployment scenarios.

For the ASA Virtual template in this example, the parameter file must have the following parameters defined:

Table 5: ASA Virtual Parameter Definitions

Field	Description	Example
vmName	The name the ASA Virtual machine will have in Azure.	cisco-asav
vmManagedImageId	The ID of the managed image used for deployment. Internally, Azure associates every resource with a Resource ID.	/subscriptions/73d2537e-ca44-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv910-Managed-Image
adminUsername	The username for logging into the ASA Virtual. This cannot be the reserved name ‘admin’.	jdoe

Field	Description	Example
adminPassword	The admin password. This must be 12 to 72 characters long, and include three of the following: 1 lower case, 1 upper case, 1 number, 1 special character.	Pw0987654321
vmStorageAccount	Your Azure storage account. You can use an existing storage account or create a new one. The storage account name must be between 3 and 24 characters, and can only contain lowercase letters and numbers.	ciscoasavstorage
virtualNetworkResourceGroup	The name of the virtual network's Resource Group. The ASA Virtual is always deployed into a new Resource Group.	ew-west8-rg
virtualNetworkName	The name of the virtual network.	ew-west8-vnet
mgmtSubnetName	The management interface will attach to this subnet. This maps to Nic0, the first subnet. Note, this must match an existing subnet name if joining an existing network.	mgmt
mgmtSubnetIP	The Management interface IP address.	10.8.0.55
gig00SubnetName	The GigabitEthernet 0/0 interface will attach to this subnet. This maps to Nic1, the second subnet. Note, this must match an existing subnet name if joining an existing network.	inside
gig00SubnetIP	The GigabitEthernet 0/0 interface IP address. This is for the ASA Virtual’s first data interface.	10.8.2.55
gig01SubnetName	The GigabitEthernet 0/1 interface will attach to this subnet. This maps to Nic2, the third subnet. Note, this must match an existing subnet name if joining an existing network.	outside

Field	Description	Example
gig01SubnetIP	The GigabitEthernet 0/1 interface IP address. This is for ASA Virtual's second data interface.	10.8.3.55
gig02SubnetName	The GigabitEthernet 0/2 interface will attach to this subnet. This maps to Nic3, the fourth subnet. Note, this must match an existing subnet name if joining an existing network.	dmz
gig02SubnetIP	The GigabitEthernet 0/2 interface IP address. This is for ASA Virtual's third data interface.	10.8.4.55
vmSize	The VM size to use for the ASA Virtual VM. Standard_D3_V2 and Standard_D3 are supported. Standard_D3_V2 is the default.	Standard_D3_V2 or Standard_D3

Create a Parameter File

You can use the example below to create your own parameter file using a text editor.

Note The following example is for IPV4 only.

Procedure

Step 1 Copy the text in the following example.

Example:

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "vmName": {
      "value": "cisco-asav1"
    },
    "vmManagedImageId": {
      "value":
"/subscriptions/33d2517e-ca88-46aa-beb2-74ff1dd61b41/resourceGroups/ewManagedImages-rg/providers/Microsoft.Compute/images/ASAv-9.10.1-81-Managed-Image"

    },
    "adminUsername": {
      "value": "jdoe"
    },
    "adminPassword": {
```

```
      "value": "Pw0987654321"
    },
    "vmStorageAccount": {
      "value": "ciscoasavstorage"
    },
    "virtualNetworkResourceGroup": {
      "value": "ew-west8-rg"
    },
    "virtualNetworkName": {
      "value": "ew-west8-vn"
    },
    "mgmtSubnetName": {
      "value": "mgmt"
    },
    "mgmtSubnetIP": {
      "value": "10.8.3.77"
    },
    "gig00SubnetName": {
      "value": "inside"
    },
    "gig00SubnetIP": {
      "value": "10.8.2.77"
    },
    "gig01SubnetName": {
      "value": "outside"
    },
    "gig01SubnetIP": {
      "value": "10.8.1.77"
    },
    "gig02SubnetName": {
      "value": "dmz"
    },
    "gig02SubnetIP": {
      "value": "10.8.0.77"
    },
    "VmSize": {
      "value": "Standard_D3_v2"
    }
  }
}
```

Step 2 Save the file locally as a JSON file; for example, **azureParameters.json**.

Step 3 Edit the file to create a template to suit your deployment parameters.

Step 4 Use this parameter template to deploy the ASA Virtual as described in Deploy the ASA Virtual from Azure Using a VHD and Resource Template, on page 19.