Deploy the Firewall Threat Defense Virtual on Azure

This chapter explains how to deploy the Secure Firewall Threat Defense Virtual from the Azure portal.

- Overview, on page 1
- Prerequisites, on page 3
- Guidelines and Limitations, on page 3
- How to Manage Secure Firewall Threat Defense Virtual Device, on page 8
- Sample Network Topology for the Firewall Threat Defense Virtual on Azure, on page 9
- Resources Created During Deployment , on page 11
- Accelerated Networking (AN), on page 12
- Azure Routing , on page 12
- Routing Configuration for VMs in the Virtual Network, on page 13
- IP Addresses, on page 13
- Deploy the Firewall Threat Defense Virtual, on page 14
- Deploy from the Azure Marketplace Using the Solution Template, on page 15
- Deploy from Azure Using a VHD and Resource Template, on page 18
- Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment, on page 21
- Upgrade Scenarios, on page 23
- Deployment of Threat Defense Virtual Cluster or Auto Scale Solution, on page 23
- Deploy the IPv6 Supported Secure Firewall Threat Defense Virtual on Azure, on page 23
- About IPv6 Supported Deployment on Azure, on page 24
- Deploy from Azure Using Custom IPv6 Template with Marketplace Image Reference, on page 25
- Deploy from Azure Using a VHD and Custom IPv6 Template, on page 31
- Firewall Threat Defense Virtual Image Snapshot, on page 35

Overview

The Secure Firewall Threat Defense Virtual is integrated into the Microsoft Azure marketplace and supports the following VM sizes:

Table 1: Azure Supported VM Sizes and Threat Defense Virtual Versions

Azure VM Size	Attributes		vNICs	Threat Defense Virtual Version
	vCPUs	Memory (GB)		
Standard_D3	4	14	4	7.7 or below
Standard_D3_v2	4	14	4	7.7 or below
Standard_D4_v2	8	28	8	6.5 to 7.7
Standard_D5_v2	16	56	8	6.5 to 7.7
Standard_D8s_v3	8	32	4	7.1 or above
Standard_D16s_v3	16	64	8	7.1 or above
Standard_F8s_v2	8	16	4	7.1 or above
Standard_F16s_v2	16	32	4	7.1 or above
Standard_D8_v4	8	32	4	7.7 or above
Standard_D16_v4	16	64	8	7.7 or above
Standard_D8s_v4	8	32	4	7.7 or above
Standard_D16s_v4	16	64	8	7.7 or above
Standard_D8_v5	8	32	4	7.7 or above
Standard_D16_v5	16	64	8	7.7 or above
Standard_D8s_v5	8	32	4	7.7 or above
Standard_D16s_v5	16	64	8	7.7 or above

Note

- By default, Threat Defense Virtual instances are deployed with Secure Boot enabled.
- From 10.0.0 onwards, only the Gen-2 instance types are supported.

Support for Deployment of Threat Defense Virtual without Diagnostic Interface on Azure

From Secure Firewall version 7.4.1, by default, the Threat Defense Virtual is deployed on Azure with 4 interfaces – 1 management, and 3 data interfaces. As the maximum number of supported interfaces is 8, you can add up to 4 more interfaces after deploying the Threat Defense Virtual to have a maximum of 8 interfaces. For example, on a Standard D4_v2 VM instance, you can deploy Threat Defense Virtual with 1 management, and 7 data interfaces.

Note The diagnostic interface is removed only on new deployments of Threat Defense Virtual instances on Azure.

Prerequisites

- A Microsoft Azure account. You can create one at https://azure.microsoft.com/en-us/ .

  After you create an account on Azure, you can log in, search the marketplace for Cisco Firepower Threat Defense, and choose the "Cisco Firepower NGFW Virtual (NGFWv)" offering.

- A Cisco Smart Account. You can create one at Cisco Software Central.

  License the Firewall Threat Defense Virtual; see *Cisco Secure Firewall Management Center Feature Licenses* for an overview of feature licenses for the firewall System, including helpful links.

- For the Firewall Threat Defense Virtual and system compatibility, see Firewall Threat Defense Virtual Compatibility.

Communication Paths

- Management interface—Used to connect the Firewall Threat Defense Virtual to the Secure Firewall Management Center.

Note In 6.7 and later, you can optionally configure a data interface for Firewall Management Center management instead of the Management interface. The Management interface is a pre-requisite for data interface management, so you still need to configure it in your initial setup. For more information about configuring a data interface for Firewall Management Center access, see the **configure network management-data-interface** command in *Cisco Secure Firewall Threat Defense Command Reference*.

- Data interfaces (required)—Used to connect the Firewall Threat Defense Virtual to inside and outside hosts.

Guidelines and Limitations

Supported Features

- Routed firewall mode only
- Azure Accelerated Networking (AN)
- Management mode, one of two choices:

- You can use the Secure Firewall Management Center to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.
- You can use the integrated Secure Firewall Device Manager to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Device Manager.

- Clustering (version 7.3 and later). For more information, see Clustering for Threat Defense Virtual in a Public Cloud.
- Public IP addressing—Assign public IP addresses to Management 0/0 and GigabitEthernet0/0.

  You can assign a public IP address to other interfaces as needed; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.
- IPv6

  The following are the guidelines and limitations that must be considered while deploying IPv6 supported Firewall Threat Defense Virtual:
  - For enabling the programmatic deployment option through the Azure CLI method for IPv6 support, pre-deployment of Firewall Threat Defense Virtual instance is not required.
  - You cannot add a Firewall Threat Defense Virtual from the Azure Marketplace to the same Vnet that you have manually upgraded from IPV4 to IPV6 addressing.
- Interfaces:
  - Firewall Threat Defense Virtual deploys with 4 vNICs by default.
  - With larger instance support, you have the ability to deploy the Firewall Threat Defense Virtual with a maximum of 8 vNICs.
  - To add additional vNICs to your Firewall Threat Defense Virtual deployment, refer to the information given in Add network interfaces to or remove network interfaces from virtual machines.
  - To change the configuration of the vNICs, or if IP forwarding is required, refer to the information given in Create, change, or delete a network interface.
  - You configure your Firewall Threat Defense Virtual interfaces using your manager. See the configuration guide for your management platform, either Firewall Management Center or Firewall Device Manager, for complete information about interface support and configuration.
- Deployment of Threat Defense Virtual without diagnostic interface-
  - When the Threat Defense Virtual is deployed without the diagnostic interface, you can configure syslog and SNMP on either the Firewall Threat Defense Virtual management interface or any of the data interfaces.
  - Clustering and auto scale deployments are supported.
  - CMI is not supported.

Note The Threat Defense virtual instance running Version 7.4.3 or later carries out several initialization tasks during its first boot, which causes the console to become available after about five minutes. This delay is normal. If the device is powered off within approximately two minutes of the first boot, important initialization steps may be interrupted, possibly leading to incomplete setup and unexpected behavior.

To resolve this issue, you must reinstall the virtual platform with a new image.

Licensing

- BYOL (Bring Your Own License) using a Cisco Smart License Account.
- PAYG (Pay As You Go) licensing, a usage-based billing model that allows customer to run Firewall Threat Defense Virtual without having to purchase Cisco Smart Licensing. All licensed features (Malware/Threat/URL Filtering/VPN, etc.) are enabled for a registered PAYG Firewall Threat Defense Virtual device. Licensed features cannot be edited or modified from the Firewall Management Center. (Version 6.5+)

Note PAYG licensing is not supported on the Firewall Threat Defense Virtual devices deployed in the Firewall Device Manager mode.

See the "Licensing" chapter in the Secure Firewall Management Center Administration Guide for guidelines when licensing your Firewall Threat Defense Virtual device.

Performance Tiers for Firewall Threat Defense Virtual Smart Licensing

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

Note Any threat defense virtual tier license can be used with any supported threat defense virtual vCPU or memory configuration.

This allows threat defense virtual customers to use a license on a wide variety of VM resources.

This can also increase the number of Azure VM sizes that are supported. When configuring a threat defense virtual VM, the maximum number of cores (vCPUs) supported is 16, and the maximum memory supported is 32 GB RAM.

Table 2: Firewall Threat Defense Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	Suggested vCPU/Memory Configuration	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250

Performance Tier	Suggested vCPU/Memory Configuration	Rate Limit	RA VPN Session Limit
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv100, 16Gbps	16 core/34 GB	16Gbps	10,000

Performance Optimizations

To achieve the best performance out of the Firewall Threat Defense Virtual, you can make adjustments to the both the VM and the host. See Virtualization Tuning and Optimization on Azure for more information.

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

Microsoft Azure Network Adapter (MANA) NIC

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.

Unsupported Features

- Licensing:
  - PLR (Permanent License Reservation)
  - PAYG (Pay As You Go) (Versions 6.4 and earlier)
- Networking (many of these limitations are Microsoft Azure restrictions):
  - Jumbo frames
  - 802.1Q VLANs
  - Transparent Mode and other Layer 2 features; no broadcast, no multicast.
  - Proxy ARP for an IP address that the device does not own from an Azure perspective (impacts some NAT capabilities).
  - Promiscuous mode (no capture of subnet traffic).
  - Inline-set modes, passive mode.

Note Azure policy prevents the Firewall Threat Defense Virtual from operating in transparent firewall or inline mode because it does not allow interfaces to operate in promiscuous mode.

- ERSPAN (uses GRE, which is not forwarded in Azure).
- Azure Outbound Access Requirement:

Note With recent Microsoft Azure changes, newly created virtual machine subnets may not have default outbound internet access.

If you experience issues with outbound connectivity from the Firewall Threat Defense Virtual, ensure that an explicit outbound access method is configured for the subnet.

Refer to the Microsoft documentation for supported outbound methods:

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/default-outbound-access#add-an-explicit-outbound-method

- Management:
  - Azure portal “reset password” function
  - Console-based password recovery; because the user does not have real-time access to the console, password recovery is not possible. It is not possible to boot the password recovery image. The only recourse is to deploy a new Firewall Threat Defense Virtual VM.
- High Availability (active/standby)
- VM import/export
- 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
- Firewall Device Manager user interface (Versions 6.4 and earlier)

Azure DDoS Protection Feature

Azure DDoS Protection in Microsoft Azure is an additional feature implemented at the forefront of the Firewall Threat Defense 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.

Snort

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

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 10.0.0 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 Threat Defense Virtual 10.0.0, you cannot roll back to a previous software version. To return to an earlier version, you must redeploy the Management Center.

How to Manage Secure Firewall Threat Defense Virtual Device

You have two options to manage your Secure Firewall Threat Defense Virtual.

Secure Firewall Management Center

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that the Firewall Threat Defense allows, use the Firewall Management Center to configure your devices instead of the integrated Firewall Device Manager. For detailed information, see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center

Important You cannot use both the Firewall Device Manager and the Firewall Management Center to manage the Firewall Threat Defense device. Once the Firewall Device Manager integrated management is enabled, it won't be possible to use the Firewall Management Center to manage the Firewall Threat Defense device, unless you disable the local management and re-configure the management to use the Firewall Management Center. On the other hand, when you register the Firewall Threat Defense device to the Firewall Management Center, the Firewall Device Manager onboard management service is disabled.

Caution Currently, Cisco does not have an option to migrate your Firewall Device Manager configuration to the Firewall Management Center and vice-versa. Take this into consideration when you choose what type of management you configure for the Firewall Threat Defense device.

Secure Firewall Device Manager

The Firewall Device Manager is a web interface included on most Firewall Threat Defense devices. It lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network with many devices. For detailed information, see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Device Manager

Note See the *Cisco Secure Firewall Threat Defense Compatibility Guide* for list of devices that support the Firewall Device Manager.

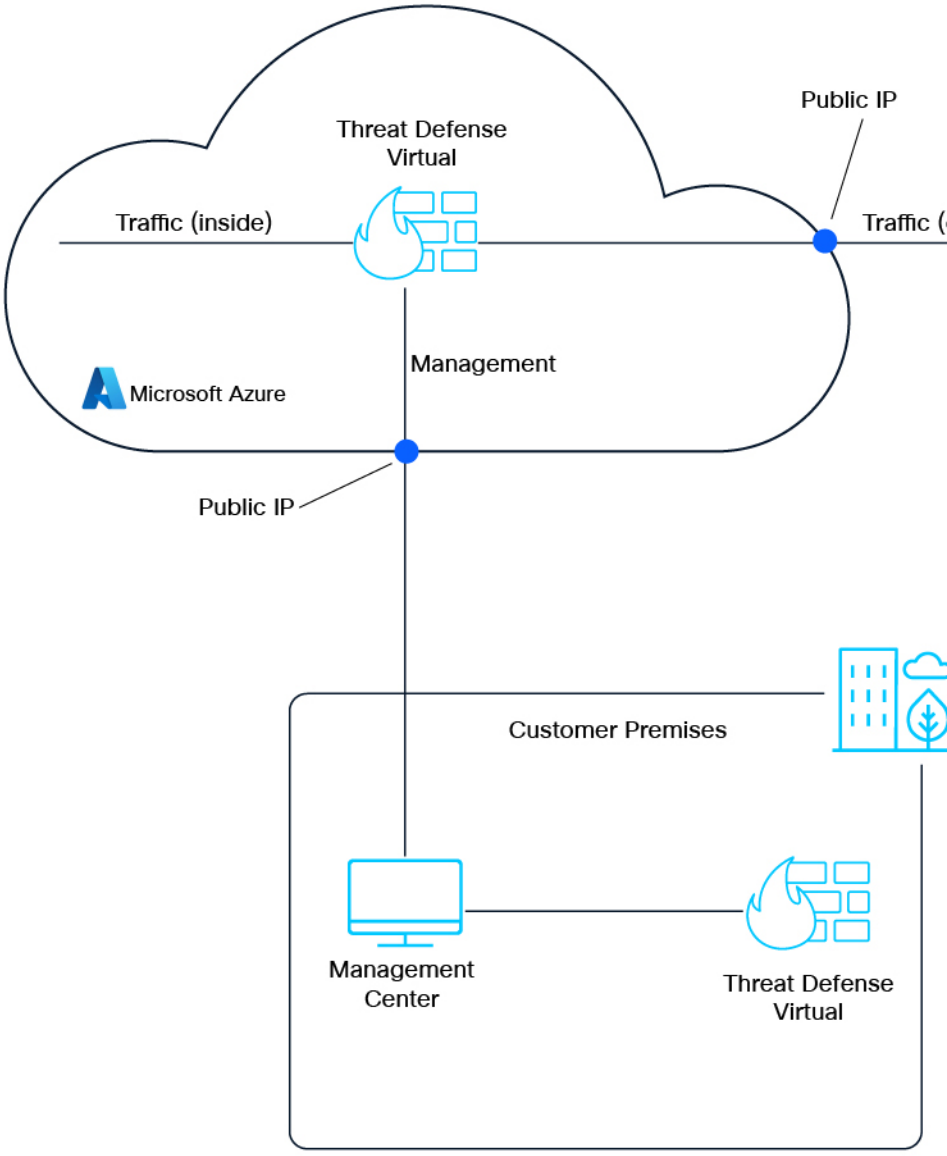
Cloud-Delivered Firewall Management Center

The Cloud-Delivered Firewall Management Center is a cloud-based management platform that allows you to centrally manage the Secure Firewall Threat Defense Virtual devices. Cloud-Delivered Firewall Management Center is supported on Secure Firewall Threat Defense Virtual versions 7.0.3, 7.2.0 and later. For detailed information, see Managing the Secure Firewall Threat Defense Virtual with the Cloud-Delivered Firewall Management Center.

Important You cannot use the Cloud-Delivered Firewall Management Center along with the Firewall Device Manager to manage the same Secure Firewall Threat Defense Virtual device.

Sample Network Topology for the Firewall Threat Defense Virtual on Azure

The following figure shows a typical topology for the Firewall Threat Defense Virtual in Routed Firewall Mode within Azure. The first defined interface is always the Management interface, and only the Management 0/0 and GigabitEthernet0/0 are assigned public IP addresses.


Public IP
Threat Defense
Virtual
Traffic (inside)
Traffic (
Management
Microsoft Azure
Public IP
Customer Premises
Management
Center
Threat Defense
Virtual

Resources Created During Deployment

When you deploy the Secure Firewall Threat Defense Virtual in Azure the following resources are created:

- The Firewall Threat Defense Virtual Machine (VM)
- A Resource Group
  - The Firewall Threat Defense Virtual is always deployed into a new Resource Group. However, you can attach it to an existing Virtual Network in another Resource Group.
- Four NICS named *vm name* -Nic0, *vm name* -Nic1, *vm name* -Nic2, *vm name* -Nic3

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

  These NICs map to the Firewall Threat Defense Virtual interfaces - Management, GigabitEthernet 0/0, GigabitEthernet 0/1, and GigabitEthernet 0/2 respectively.

- A security group named *vm name* -mgmt-SecurityGroup

  The security group will be attached to the VM's Nic0, which maps to the Firewall Threat Defense Virtual management interface.

  The security group includes rules to allow SSH (TCP port 22) and the management traffic for the Firewall Management Center interface (TCP port 8305). 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 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 will be created if you choose the New Network option.
- A Routing Table for each subnet (updated if it already exists)

  The tables are named "*subnet name* "-FTDv-RouteTable.

  Each routing table includes routes to the other three subnets with the Firewall Threat Defense 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.

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.

Limitations of using ixgbe-vf Interfaces

Be aware of the following limitations when using ixgbe-vf interfaces:

- The guest VM is not allowed to set the VF to promiscuous mode. Because of this, transparent mode is not supported when using ixgbe-vf.
- The guest VM is not allowed to set the MAC address on the VF. Because of this, the MAC address is not transferred during HA like it is done on other Firewall Threat Defense Virtual platforms and with other interface types. HA failover works by transferring the IP address from active to standby.

Note This limitation is applicable to the i40e-vf interfaces too.

- The Cisco UCS-B server does not support the ixgbe-vf vNIC.
- In a failover setup, when a paired Firewall Threat Defense Virtual (primary unit) fails, the standby unit takes over as the primary unit role and its interface IP address is updated with a new MAC address of the standby Firewall Threat Defense Virtual unit. Thereafter, the Firewall Threat Defense Virtual sends a gratuitous Address Resolution Protocol (ARP) update to announce the change in MAC address of the interface IP address to other devices on the same network. However, due to incompatibility with these types of interfaces, the gratuitous ARP update is not sent to the global IP address that is defined in the NAT or PAT statements for translating the interface IP address to global IP addresses.

Azure Routing

Routing in an Azure Virtual Network Subnet is determined by the Subnet's Effective Routing Table. The Effective Routing Table is a combination of built-in system routes and the routes in the User Defined Route (UDR) Table.

Note You can view the Effective Routing Table under VM NIC properties.

You can view and edit the User Defined Routing table. When the system routes and the user defined routes 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) IPv4 or [::/0] IPv6 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 Azure Routing Firewall Threat Defense Virtual, routes must be added/updated in the User Defined Routing table associated with each data subnet. Traffic of interest should be routed by using the Firewall Threat Defense Virtual IP address on that subnet as the next-hop. Also, a default route for 0.0.0.0/0 IPv4 or [::/0] IPv6 can be added with a next hop of the Firewall Threat Defense Virtual IP if needed.

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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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.

IP Addresses

The following information applies to IP addresses in Azure:

- The first NIC on the Firewall Threat Defense Virtual (which maps to Management) 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 handles the NAT translations.

  You can associate a public IP address with a data interface (GigabitEthernet0/0, for example) after the Firewall Threat Defense Virtual has been deployed; see Public IP addresses for Azure's guidelines regarding public IPs, including how to create, change, or delete a public IP address.

- You can enable **IP Forwarding** in the network interface attached to a Firewall Threat Defense 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 (IPv4 and IPv6) are dynamic and may change during an Azure stop/start cycle. However, they are persistent during Azure restart and during Firewall Threat Defense Virtual reload. See IPv6 Public IP Address Standards.
- Public IP addresses that are static do not change until you change them in Azure.
- Firewall Threat Defense Virtual interfaces may use DHCP to set their IP addresses. The Azure infrastructure ensures that the Firewall Threat Defense Virtual interfaces are assigned the IP addresses set in Azure.

Deploy the Firewall Threat Defense Virtual

You can deploy the Firewall Threat Defense Virtual in Azure using templates. Cisco provides two kinds of templates:

- **Solution Template in the Azure Marketplace**—Use the solution template available in the Azure Marketplace to deploy the Firewall Threat Defense Virtual using the Azure portal. You can use an existing resource group and storage account (or create them new) to deploy the virtual appliance. To use the solution template, see Deploy from the Azure Marketplace Using the Solution Template, on page 15.
- **Custom Template using a Managed Image from a VHD (available from** https://software.cisco.com/download/home)—In addition to the Marketplace-based deployment, Cisco provides a compressed virtual hard disk (VHD) that you can upload to Azure to simplify the process of deploying the Firewall Threat Defense Virtual in Azure. Using a Managed Image and two JSON files (a Template file and a Parameters File), you can deploy and provision all the resources for the Firewall Threat Defense Virtual in a single, coordinated operation. To use the custom template, see Deploy from Azure Using a VHD and Resource Template, on page 18.

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 Threat Defence Virtual - BYOL and PAYG
- Cisco Secure Firewall Threat Defence for Azure Virtual WAN

Deploy from the Azure Marketplace Using the Solution Template

The following instructions show you how to deploy the solution template for the Firewall Threat Defense Virtual that is available in the Azure Marketplace. This is a top-level list of steps to set up the Firewall Threat Defense Virtual in the Microsoft Azure environment. For detailed steps about the Azure setup, see Getting Started with Azure.

When you deploy the Firewall Threat Defense Virtual in Azure, it automatically generates various configurations, such as resources, public IP addresses (IPv4 and IPv6), 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.

Note To use the customizable ARM templates available in the GitHub repository, see Deploy from Azure Using a VHD and Resource Template, on page 18.

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 Choose **Azure Marketplace** > **Virtual Machines**.

Step 3 Search Marketplace for "Cisco Firepower NGFW Virtual (Firewall Threat Defense Virtual)", choose the offering, and click **Create**.

Step 4 Configure the basic settings.

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

Important
If you use an existing name the deployment will fail.

b) Choose your licensing method, either **BYOL** or **PAYG**.

Choose **BYOL** (Bring Your Own License) to use a Cisco Smart License Account.

Choose **PAYG** (Pay As You Go) licensing to use a usage-based billing model without having to purchase Cisco Smart Licensing.

Important
PAYG licensing is supported only when the Firewall Threat Defense Virtual is managed using Firewall Management Center.

FDM-managed deployments are not supported with **PAYG** licensing and must use **BYOL** instead.

c) Enter a username for the Firewall Threat Defense Virtual administrator.

Note
The name "admin" is reserved in Azure and cannot be used.

d) Choose an authentication type, either password or SSH key.

If you choose password, enter a password and confirm.

If you choose SSH key, specify the RSA public key of the remote peer.

e) Create a password to use with the **Admin** user account when you log in to configure the Firewall Threat Defense Virtual.

f) Select the management center you want to register the Firewall Threat Defense Virtual from the **FTDv Management** drop-down list.

If you are choosing **FMC: Firepower Management Center** as the management center for your device, using the following option you can configure the management center for your device.

- Click **Yes** to enter the **FMC registration information**.
  1. Enter the **FMC IP** address.
  2. Enter the **FMC Registration Key** for registering the Threat Defense Virtual instances.
  3. [Optional] Enter the management center NAT ID that is used during instance registration.

g) If you are using the virtual machine you are deploying as a cluster, then click **Yes (provide day0 cluster configuration)** to create and enter the basic day0 configuration details.

- Enter the day0 configuration details in the **Day0 cluster configuration** field.

  For information on creating day0 configuration for Azure, see Create the Day0 Configuration for Azure in the Deploy a Threat Defense Virtual Cluster on Azure guide.

  Note
  You can only configure the partial day0 config (cluster config): "Cluster": {...} OR "run_config": [...] details.

h) Choose your subscription.

i) Create a new Resource Group.

The Firewall Threat Defense Virtual should be deployed into a new Resource Group. The option to deploy into an existing Resource Group only works if that existing Resource Group is empty.

However, you can attach the Firewall Threat Defense Virtual to an existing Virtual Network in another Resource Group when configuring the network options in later steps.

j) Select geographical location. This should be the same for all resources used in this deployment (for example: Firewall Threat Defense Virtual, Network, storage accounts).

k) Click **OK**.

Step 5 Configure the Firewall Threat Defense Virtual settings.

a) Choose the virtual machine size.

b) Choose a storage account.

Note
You can use an existing storage account or create a new one. The storage account name can only contain lowercase letters and numbers.

c) Choose a public IP address.

You can choose a public IP address available for the selected subscription and location, or click **Create new**.

When you create a new public IP address, you get one from the block of IP addresses that Microsoft owns, so you can't choose a specific one. The maximum number of public IP addresses you can assign to an interface is based on your Azure subscription.

Important
Azure creates a dynamic public IP address by default. The public IP may change when the VM is stopped and restarted. If you prefer a fixed IP address, you should create a static address. You can also modify the public IP address after deployment and change it from a dynamic to a static address.

In case the VM needs to assign the public IPv6 address, refer to the IPv6 standards IPv6 Public IP Address Standards.

d) Add the DNS label.

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

e) Choose a virtual network.

You can choose an existing Azure Virtual Network (VNet) or create a new one and enter the IP address space for the VNet. By default, the Classless Inter-Domain Routing (CIDR) IP address is 10.0.0.0/16.

If the Virtual Machine is required for the IPv6 addressing, you need to enable it in the virtual network. Example: By default, the CIDR IPv6 address is [ace:cab:deca::/48].

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. For more information on IPv6, see Azure IPv6 Overview

f) Configure four subnets for the Firewall Threat Defense Virtual network interfaces:

- **FTDv Management** interface, attached to Nic0 in Azure, the "First subnet"
- **FTDv Data** interface 1, attached to Nic1 in Azure, the "Second subnet"
- **FTDv Data** interface 2, attached to Nic2 in Azure, the "Third subnet"
- **FTDv Data** interface 3, attached to Nic3 in Azure, the "Fourth subnet"

Note
For the above subnets, if we require IPv6 configuration while creating the subnets, select the IPv6 option and configure IPv6 subnets for the interface.

g) Provide **Public inbound ports (mgmt.interface)** input to indicate whether any ports are to be opened for public or not. By default, **None** is selected.

- Click **None** to create and attach a network security group with Azure's default security rule to the management interface. Selecting this option allows traffic from sources in the same virtual network and from the Azure load balancer.
- Click **Allow selected ports** to view and choose the inbound ports to be opened for acess by the internet. Choose any of the following ports from the **Select Inbound Ports** drop-down list. By default, **SSH (22)** is selected.
  - SSH (22)
  - SFTunnel (8305)
  - HTTPs (443)

h) Click **OK**.

Step 6 View the configuration summary, and then click **OK**.

Step 7 View the terms of use and then click **Purchase**.

Deployment times vary in Azure. Wait until Azure reports that the Firewall Threat Defense Virtual VM is running.

Warning
After deployment, the Firewall Threat Defense Virtual begins its firstboot initialization process. Do not shut down, reboot, or modify the VM during this time.

Interrupting firstboot can leave the system in an inconsistent state and may require redeployment. Ensure that firstboot has fully completed before making any configuration changes.

What to do next

Your next steps depend on what management mode you chose.

- If you chose **No** for **Enable Local Manager**, you'll use the Secure Firewall Management Center to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.
- If you chose **Yes** for **Enable Local Manager**, you'll use the integrated Secure Firewall Device Manager to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Device Manager.

See How to Manage Secure Firewall Threat Defense Virtual Device for an overview of how to choose your management option.

Deploy from Azure Using a VHD and Resource Template

You can create your own custom Firewall Threat Defense 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 Firewall Threat Defense Virtual template deployment. You can download these files from the Github repository.
- This procedure requires an existing Linux VM in Azure. We recommend that 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 time to Azure storage is 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 Firewall Threat Defense Virtual.

Procedure

Step 1 Download the Firewall Threat Defense Virtual compressed VHD image from the Cisco Download Software page:

a) Navigate to **Products** > **Security** > **Firewalls** > **Next-Generation Firewalls (NGFW)** > **Secure Firewall Threat Defense Virtual**.

b) Click **Firepower Threat Defense Software**.

Follow the instructions for downloading the image.

For example, Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.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/Cisco_Secure_Firewall_Threat_Defense_Virtual-7.1.0-92.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 Firewall Threat Defense 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 Cisco_Firepower_Threat_Defense_Virtual-7.1.0-92.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 Firewall Threat Defense Virtual VHD.

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 Firewall Threat Defense 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 a Firewall Threat Defense Virtual firewall using the managed image and a resource template:

a) On the Azure GUI, search for **Custom deployment**.
b) Under **Select a template**, click **Build your own template in the editor**.

You have a blank template that is available for customizing. See Github for the template files.

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

h) To deploy the Threat Defense Virtual without the diagnostic interface, enter a day-0 configuration script that includes the key-value pair **Diagnostic: OFF** in the Custom Data field. A sample day-0 configuration script is given below.

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

Note
The key value pair, "Diagnostic": "ON/OFF", is case-sensitive.

You can also modify the script in the Custom Data field in the ARM template that is used for fresh deployment.

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 Firewall Threat Defense Virtual parameter file. See Github for the template parameters.

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 a Firewall Threat Defense 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

- Update the Firewall Threat Defense Virtual's IP configuration in Azure.

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 Threat Defense Virtual VM Offers (used for both the Cisco Secure Firewall Threat Defense Virtual Application offers)
  - Offer ID: **cisco-ftdv**
  - BYOL Plan ID: **ftdv-azure-byol**

- PAYG Plan ID: **ftdv-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 Threat Defense 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-ftdv'
  SpecificPlanIdsLimitation =@('ftdv-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.

Upgrade Scenarios

You can upgrade a Firewall Threat Defense Virtual instance as per the scenarios given below.

- Secure firewall version 7.3 and earlier – You can upgrade a Firewall Threat Defense Virtual instance deployed with a diagnostic interface to a Firewall Threat Defense Virtual instance with a diagnostic interface.
- Secure Firewall version 7.4.1 and later – You can upgrade a Firewall Threat Defense Virtual instance deployed without a diagnostic interface to a Firewall Threat Defense Virtual instance without a diagnostic interface.

The upgrade scenario given below is not supported.

- All Secure firewall versions – You cannot upgrade a Firewall Threat Defense Virtual instance deployed with a diagnostic interface to a Firewall Threat Defense Virtual instance without a diagnostic interface.

Note The number and order of the NICs is maintained after upgrading.

Deployment of Threat Defense Virtual Cluster or Auto Scale Solution

The deployment of a Firewall Threat Defense Virtual cluster or an auto scale solution requires four network interfaces—one management interface and three data interfaces—which are assigned during the Azure Marketplace deployment. No additional configuration is required in the Day-0 configuration script.

Deploy the IPv6 Supported Secure Firewall Threat Defense Virtual on Azure

This chapter explains how to deploy the IPv6 Supported Firewall Threat Defense Virtual from the Azure portal.

About IPv6 Supported Deployment on Azure

Firewall Threat Defense Virtual offerings support both IPV4 and IPv6 from 7.3 and later. In Azure, you can deploy Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense Virtual . See, Deploy from Azure Using a VHD and Custom IPv6 Template, on page 31.

The process involved in deploying Firewall Threat Defense 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 Firewall Threat Defense Virtual is as follows:

Table 3:

Step	Process

1	Create a Linux VM in Azure where you are planning to deploy the IPv6-supported Firewall Threat Defense Virtual
2	Enable Programmatic deployment option on Azure portal or Azure CLI **only** when you are deploying Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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 Firewall Threat Defense 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-ftdv'
- **<sku/plan>** - 'ftdv-azure-byol'

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

- **az vm image terms show -p cisco -f cisco-ftdv --plan ftdv-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-ftdv'
- **<sku>** - 'ftdv-azure-byol'

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

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

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

For IPv6 support deployment of Firewall Threat Defense Virtual , you must select the Firewall Threat Defense Virtual version as 73* 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 Firewall Threat Defense Virtual custom deployment:

Parameter Name	Examples of allowed Values/Type	Description
vmName	csf-tdv	Name the Firewall Threat Defense Virtual VM in Azure.

Parameter Name	Examples of allowed Values/Type	Description
softwareVersion	730.33.0	The software version of the marketplace image version.
billingType	BYOL	The licensing method is BYOL or PAYG. BYOL license is more cost effective compared to PAYG, hence it is recommended to opt for BYOL subscribed deployment.
adminUsername	hjohn	The username to log into Firewall Threat Defense 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. 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).

Parameter Name	Examples of allowed Values/Type	Description
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\":\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	The field to provide in the Day 0 configuration to the Firewall Threat Defense Virtual . By default it has the following three key-value pairs to configure: • 'admin' user password • Firewall Management Center Virtual hostname • the Firewall Management Center Virtual 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 Firewall Management Center Virtual as Firewall Threat Defense Virtual manager and also give the inputs for fields required to configure the same on Firewall Management Center Virtual.
virtualNetworkResourceGroup	cisco-tdv-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-tdv-vent	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'.

Parameter Name	Examples of allowed Values/Type	Description
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'.
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'.

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

Step 7 Use the ARM template to deploy Firewall Threat Defense 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

Your next steps depend on what management mode you chose.

- If you chose **No** for **Enable Local Manager**, you'll use the Secure Firewall Management Center to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.
- If you chose **Yes** for **Enable Local Manager**, you'll use the integrated Secure Firewall Device Manager to manage your Firewall Threat Defense VirtualFirewall Threat Defense VirtualFirewall Threat Defense VirtualFirewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall device manager.

  See How to Manage Your Secure Firewall Threat Defense Virtual Device for an overview of how to choose your management option.

Deploy from Azure Using a VHD and Custom IPv6 Template

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

Before you begin

- You need the JSON template and corresponding JSON parameter file for your Firewall Threat Defense 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 Firewall Threat Defense Virtual .

Procedure

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

a) Navigate to **Products** > **Security** > **Firewalls** > **Next-Generation Firewalls (NGFW)** > **Secure Firewall Threat Defense Virtual**.

b) Click **Firepower Threat Defense Software**.

Follow the instructions for downloading the image.

Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

Step 2 Perform **Step 2** through **Step 8** in Deploy 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 Firewall Threat Defense Virtual parameter file. See the sample for the Azure Firewall Threat Defense 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 Firewall Threat Defense Virtual deployment:

Parameter Name	Examples of allowed values/types	Description
vmName	csf-tdv	Name the Firewall Threat Defense 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 Firewall Threat Defense 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. 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).
customData	{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}	The field to provide in the Day 0 configuration to the Firewall Threat Defense Virtual . By default it has the following three key-value pairs to configure: • 'admin' user password • CSF-MCv hostname

Parameter Name	Examples of allowed values/types	Description
		• 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	csf-tdv	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	hjohn-vm-vn	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.

Parameter Name	Examples of allowed values/types	Description
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 '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 Firewall Threat Defense Virtual VM. Standard_D3_v2 is the default.

Step 4 Use the ARM template to deploy Firewall Threat Defense 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

- Update the Firewall Threat Defense Virtual's IP configuration in Azure.

Firewall Threat Defense Virtual Image Snapshot

You can create and deploy the Firewall Threat Defense Virtual using a snapshot image in the Azure portal. The image snapshot is a replicated Firewall Threat Defense Virtual image instance with no state data.

Firewall Threat Defense Virtual Snapshot Overview

The process of creating a snapshot image of the Firewall Threat Defense Virtual instance helps to minimize the initial system *init* time by skipping the first boot procedures done for the Firewall Threat Defense Virtual and FSIC. The snapshot image consists of prepopulated database and the Firewall Threat Defense Virtual initial boot process, which enables the image to regenerate unique IDs (UUIDs, Serial number) that is related to the system identity in the Firewall Management Center or any other management center. This process helps in faster boot time of Firewall Threat Defense Virtual, which is essential in auto scale deployment.

Note Snapshot image creation is used to minimize the initial system init time on a non-registered Secure Firewall Threat Defense Virtual. It should not be used for the purpose of *backup/restore*.

Note Currently, Pay-As-You-Go (PAYG) licensing is not supported for instances deployed using a snapshot image of the Firewall Threat Defense Virtual. PAYG licensing is only available for instances that you deploy directly from the Marketplace. You can use Smart Licensing for such new Firewall Threat Defense Virtual deployments with PAYG licensing.

Create the Firewall Threat Defense Virtual Snapshot Image from Managed Image

Firewall Threat Defense Virtual image snapshot creation is a process of replicating an existing managed image of the Firewall Threat Defense Virtual instance in the Azure portal.

Before you begin

You must have created a managed image of the Firewall Threat Defense Virtual version 7.2 or later by uploading the resized VHD image to a container in your Azure storage account of a Linux VM in the Azure

portal. For information on creating resized VHD image, see Deploy from Azure Using a VHD and Resource Template, on page 18.

You must not register the Firewall Threat Defense Virtual instance you are preparing for image snapshot to any manager such as the Firewall Management Center or the Firewall Device Manager.

Procedure

Step 1 Go to Azure portal where you have created the managed image of the Firewall Threat Defense Virtual instance.

Note
Ensure that the Firewall Threat Defense Virtual instance which you are planning to replicate is not registered to the Firewall Management Center or configured to any other local manager or applied with any configuration.

Step 2 Go to **Resource Group** and select the Firewall Threat Defense Virtual instance.

Step 3 Click the **Serial Console** on the navigation page of the Firewall Threat Defense Virtual instance.

Step 4 Use the following scripts to run the pre-snapshot process from the expert shell:

```
> expert
admin@FTDvbaseimg:~$ Sudo su
root@firepower:/ngfw/var/common# prepare_snapshot
Do you want to continue [Y/N]:
```

When you use `prepare_snapshot` command in the script, an intermediate message appears prompting for confirmation to execute the script. Press **Y** to run the script.

Alternatively, you can append `-f` to this command, such as `root@firepower:/ngfw/var/common# prepare_snapshot -f` to skip the user confirmation message and directly execute the script.

This script removes all the line configurations, deployed policies, configured manager, UUIDs associated with the Firewall Threat Defense Virtual instance. After the processing is done, the Firewall Threat Defense Virtual instance is shut down.

Step 5 Click **Capture**.

Step 6 In the **Create an image** page, choose an existing resource group or create a new one from the **Resource Group** drop-down list.

Step 7 Click **No, capture only a managed image** in the **Instance Details** section to create only a managed image.

Step 8 Provide name for the snapshot image you are creating using the managed image of the Firewall Threat Defense Virtual instance.

Step 9 Click **Review+Create** to create a new snapshot image of the Firewall Threat Defense Virtual instance.

What to do next

Deploy the Firewall Threat Defense Virtual instance using snapshot image. See Deploy Secure Firewall Threat Defenece Virtual using snapshot image.

Deploy the Firewall Threat Defense Virtual Instance using Image Snapshot

Before you begin

Cisco recommends the following:

- Confirm that a snapshot image is available for the Firewall Threat Defense Virtual instance.

Procedure

Step 1 Log in to Azure portal.

Step 2 Copy the Resource ID of the newly created snapshot image.

Note
Azure associates every resource (snapshot image) with a Resource ID. The Resource ID of the snapshot image is required for deploying the new Firewall Threat Defense Virtual instance.

a) In the Azure Portal, select **Images**.
b) Select the snapshot image you have created by using a managed image.
c) Click **Overview** to view the image properties.
d) Copy the **Resource ID** to the clipboard. The **Resource ID** syntax is represented as: **/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>**

Step 3 Continue deploying the Firewall Threat Defense Virtual instance using the snapshot image. See Deploy from Azure Using a VHD and Resource Template, on page 18.

Note
You can run the CLI commands **show version** and **show snapshot detail** from the Firewall Threat Defense Virtual console to know about the version and details of the newly deployed Firewall Threat Defense Virtual instance.