Deploy the Threat Defense Virtual on Azure

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

Overview

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

- Standard D3—4 vCPUs, 14 GB, 4vNICs
- Standard D3_v2—4 vCPUs, 14 GB, 4vNICs
- Standard D4_v2—8 vCPUs, 28 GB, 8vNICs (**New in Version 6.5**)
- Standard D5_v2—16 vCPUs, 56 GB, 8vNICs (**New in Version 6.5**)
- Standard_D8s_v3—8 vCPUs, 32 GB, 4vNICs (**New in Version 7.1**)
- Standard_D16s_v3—16 vCPUs, 64 GB, 8vNICs (**New in Version 7.1**)
- Standard_F8s_v2—8 vCPUs, 16 GB, 4vNICs (**New in Version 7.1**)
- Standard_F16s_v2—16 vCPUs, 32 GB, 4vNICs (**New in Version 7.1**)

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 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 threat defense virtual and system compatibility, see Threat Defense Virtual Compatibility.

Communication Paths

- Management interface—Used to connect the threat defense virtual to the Secure Firewall Management Center.

Note In 6.7 and later, you can optionally configure a data interface for 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 management center access, see the **configure network management-data-interface** command in Cisco Secure Firewall Threat Defense Command Reference.

- Diagnostic interface—Used for diagnostics and reporting; cannot be used for through traffic.
- Inside interface (required)—Used to connect the threat defense virtual to inside hosts.

- Outside interface (required)—Used to connect the threat defense virtual to the public network.
- From Secure Firewall version 7.4.1, you can remove the diagnostic interface and deploy the Threat Defense Virtual on Azure with a minimum of 3 interfaces – 1 management, and 2 data interfaces. We recommend that you deploy the Threat Defense Virtual on Azure without the diagnostic interface from Secure Firewall version 7.4.1. For more information, see About Deployment of Threat Defense Virtual without Diagnostic Interface on Azure, on page 19.

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 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 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 threat defense virtual:
  - For enabling the programmatic deployment option through the Azure CLI method for IPv6 support, pre-deployment of threat defense virtual instance is not required.
  - You cannot add a threat defense virtual from the Azure Marketplace to the same Vnet that you have manually upgraded from IPV4 to IPV6 addressing.
- Interfaces:
  - Threat Defense Virtual deploys with 4 vNICs by default.
  - With larger instance support, you have the ability to deploy the threat defense virtual with a maximum of 8 vNICs.
  - To add additional vNICs to your 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 threat defense virtual interfaces using your manager. See the configuration guide for your management platform, either management center or device manager, for complete information about interface support and configuration.

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 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 threat defense virtual device. Licensed features cannot be edited or modified from the management center. (Version 6.5+)

Note PAYG licensing is not supported on the threat defense virtual devices deployed in the device manager mode.

See the "Licensing" chapter in the Secure Firewall Management Center Administration Guide for guidelines when licensing your threat defense virtual device.

Performance Tiers for Threat Defense Virtual Smart Licensing

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

Table 1: Threat Defense Virtual Licensed Feature Limits Based on Entitlement

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
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 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 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.

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 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).
- 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 threat defense virtual VM.
- High Availability (active/standby)
- VM import/export
- Gen 2 VM generation on Azure
- 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
- 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 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 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 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.

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 threat defense allows, use the management center to configure your devices instead of the integrated device manager.

Important You cannot use both the device manager and the management center to manage the threat defense device. Once the device manager integrated management is enabled, it won't be possible to use the management center to manage the threat defense device, unless you disable the local management and re-configure the management to use the management center. On the other hand, when you register the threat defense device to the management center, the device manager onboard management service is disabled.

Caution Currently, Cisco does not have an option to migrate your device manager configuration to the management center and vice-versa. Take this into consideration when you choose what type of management you configure for the threat defense device.

Secure Firewall device manager

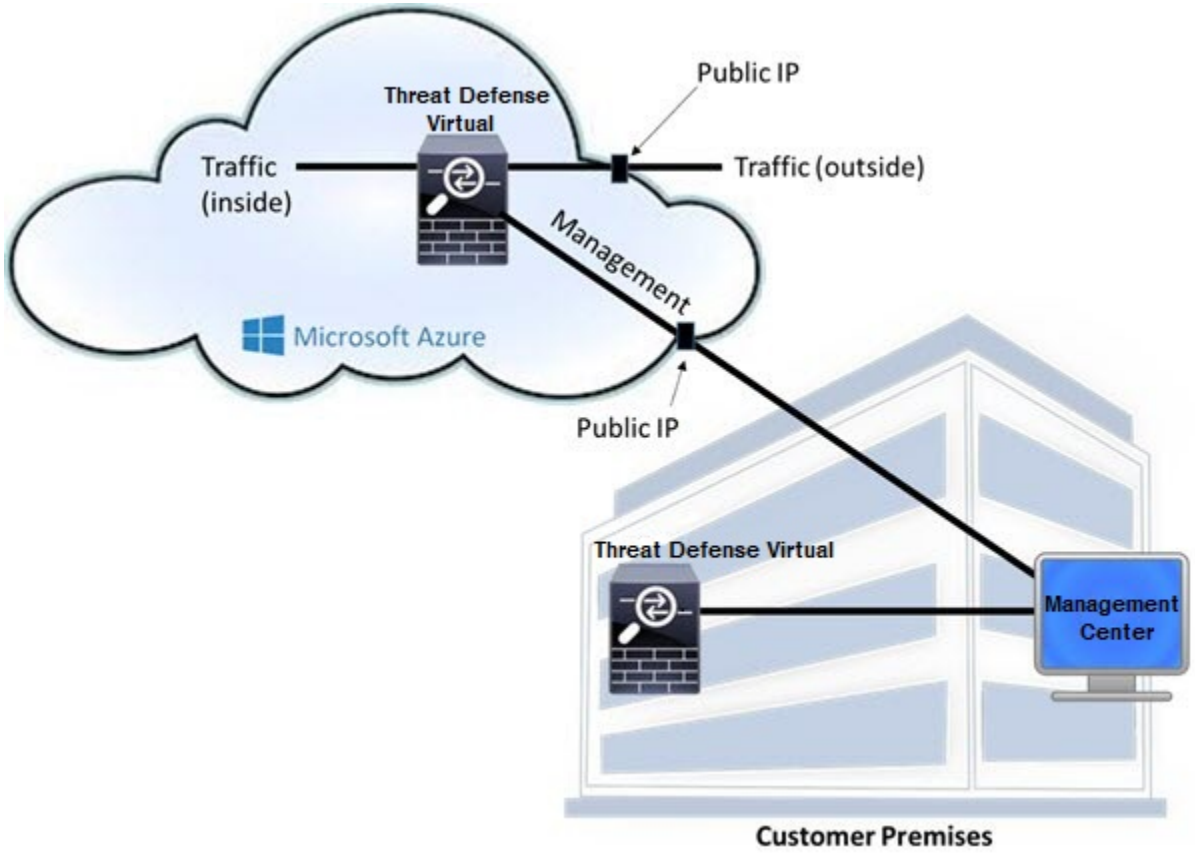
The device manager is an onboard integrated manager.

The device manager is a web-based configuration interface included on some of the threat defense devices. The device manager 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 containing many of the threat defense devices.

Note See the Cisco Secure Firewall Device Manager Configuration Guide for list of the threat defense devices that support the device manager.

Sample Network Topology for the Threat Defense Virtual on Azure

The following figure shows a typical topology for the 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.



Resources Created During Deployment

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

- The threat defense virtual Machine (VM)
- A Resource Group

- The 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 threat defense virtual interfaces Management, Diagnostic 0/0, GigabitEthernet 0/0, and GigabitEthernet 0/1 respectively.

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

  The security group will be attached to the VM's Nic0, which maps to the threat defense virtual management interface.

  The security group includes rules to allow SSH (TCP port 22) and the management traffic for the 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 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 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 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 threat defense virtual unit. Thereafter, the 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 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 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 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 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 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 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 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 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 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 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.

- Threat Defense Virtual interfaces may use DHCP to set their IP addresses. The Azure infrastructure ensures that the threat defense virtual interfaces are assigned the IP addresses set in Azure.

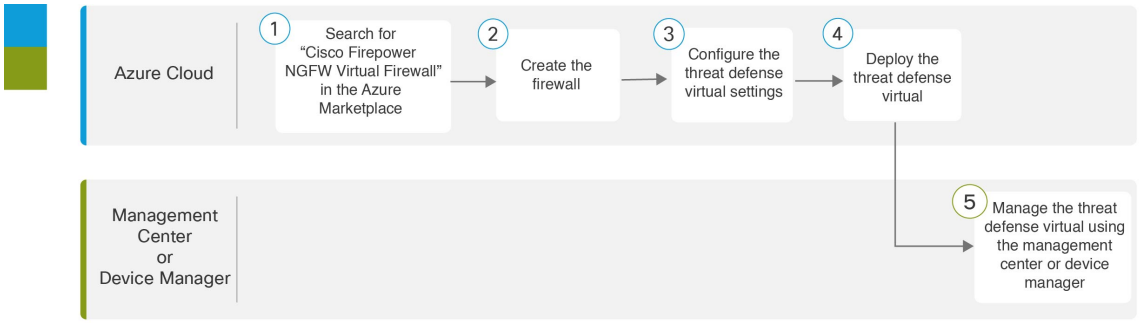
Deploy the Threat Defense Virtual

You can deploy the 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 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 13.
- **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 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 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 16.

End-to-End Procedure

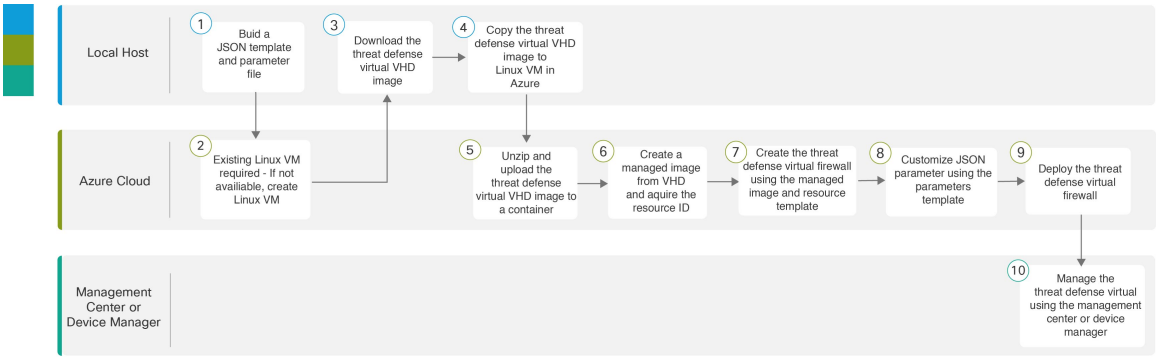
The following flowchart illustrates the workflow for deploying the threat defense virtual on Microsoft Azure using the Solution template.



	Workspace	Steps
1	Azure Cloud	Deploy from the Azure Marketplace Using the Solution Template: Search for "Cisco Firepower NGFW Virtual Firewall" in the Azure Marketplace.
2	Azure Cloud	Deploy from the Azure Marketplace Using the Solution Template: Create the firewall.
3	Azure Cloud	Deploy from the Azure Marketplace Using the Solution Template: Configure the threat defense virtual settings.
4	Azure Cloud	Deploy from the Azure Marketplace Using the Solution Template: Deploy the threat defense virtual.

	Workspace	Steps
5	Management Center or Device Manager	Manage the threat defense virtual: • Managing the Threat Defense Virtual with the Management Center • Managing the Threat Defense Virtual with the Device Manager

The following flowchart illustrates the workflow for deploying the threat defense virtual on Microsoft Azure using a VHD and Resource template.



	Workspace	Steps
1	Local Host	Deploy from Azure Using a VHD and Resource Template: Build a JSON template and parameter file.
2	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Existing Linux VM required - if not available, create a Linux VM: • Create a Linux virtual machine with the Azure CLI • Create a Linux virtual machine with the Azure portal
3	Local Host	Deploy from Azure Using a VHD and Resource Template: Download the threat defense virtual VHD image from the Cisco Download Software page.
4	Local Host	Deploy from Azure Using a VHD and Resource Template: Copy the threat defense virtual VHD image to Linux VM in Azure.
5	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Unzip and upload the threat defense virtual VHD image to a container.
6	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Create a managed image from VHD and acquire the Resource ID of that image.
7	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Create the threat defense virtual firewall using the managed image and a resource template.
8	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Customize JSON parameters using the parameters template.

	Workspace	Steps
9	Azure Cloud	Deploy from Azure Using a VHD and Resource Template: Deploy the threat defense virtual firewall.
10	Management Center or Device Manager	Manage the threat defense virtual: • Managing the Threat Defense Virtual with the Management Center • Managing the Threat Defense Virtual with the Device Manager

Deploy from the Azure Marketplace Using the Solution Template

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

When you deploy the 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 16.

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 (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
You can only use **PAYG** when you manage the threat defense virtual using the management center.

c) Enter a username for the 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 threat defense virtual.

f) Select the management center you want to register the 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 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 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: Threat Defense Virtual, Network, storage accounts).

k) Click **OK**.

Step 5 Configure the 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 threat defense virtual network interfaces:

- **FTDv Management** interface, attached to Nic0 in Azure, the "First subnet"
- **FTDv Diagnostic** interface, attached to Nic1 in Azure, the "Second subnet"
- **FTDv Outside** interface, attached to Nic2 in Azure, the "Third subnet"
- **FTDv Inside** interface, 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 threat defense virtual VM is running.

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 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 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 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 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 Threat Defense Virtual.

Procedure

Step 1 Download the 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 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 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 **Gen 1**.

  Note
  Gen 2 is not supported.

- **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 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 Threat Defense 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 Github for the template files.

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 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 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 Threat Defense Virtual's IP configuration in Azure.

About Deployment of Threat Defense Virtual without Diagnostic Interface on Azure

On Secure Firewall version 7.3 and earlier, the Threat Defense Virtual is deployed with a minimum of 4 interfaces –1 management, 1 diagnostic, and 2 data interfaces.

From Secure Firewall version 7.4.1, you can remove the diagnostic interface and deploy the Threat Defense Virtual with a minimum of 3 interfaces – 1 management, and 2 data interfaces. This feature enables deployment of Threat Defense Virtual with an additional data interface on the same instance type. For example, on a Standard D4_v2 VM instance, instead of deploying Threat Defense Virtual with 1 management, 1 diagnostic, and 6 data interfaces, you can now deploy Threat Defense Virtual with 1 management, and 7 data interfaces.

From Secure Firewall version 7.4.1, we recommend that you deploy the Threat Defense Virtual on Azure without the diagnostic interface.

This feature is supported only on new deployments of Threat Defense Virtual instances on Azure.

Note As the maximum number of supported interfaces is 8, you can add up to 5 more interfaces after deploying the Threat Defense Virtual to have a maximum of 8 interfaces.

Guidelines and Limitations for Deployment of Threat Defense Virtual without Diagnostic Interface on Azure

- When the diagnostic interface is removed, syslog and SNMP is supported using either the Threat Defense Virtual management or the data interface instead of the diagnostic interface.
- Clustering and auto scale is supported with this deployment.

- Grouping of Threat Defense Virtual instances with diagnostic interface port and Threat Defense Virtual instances without diagnostic interface port is not supported.

Note The grouping of Threat Defense Virtual instances here refers to the grouping of the instances in the Virtual Machine Scale Set (VMSS) on Azure. This does not pertain to the grouping of Threat Defense Virtual instances on the Management Center Virtual.

- CMI is not supported.

NIC Mapping to Data Interfaces for Deployment of Threat Defense Virtual without Diagnostic Interface on Azure

The NIC mapping to data interfaces for deployment of Threat Defense Virtual without the diagnostic interface on Azure is given below.

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	diag-subnet	M0/0*
NIC2	inside-subnet	Gig0/0
NIC3	outside-subnet	Gig0/1

Threat Defense Virtual-4-NICs

*Diagnostic interface

Net-Interface	Vnet/Subnet	Port
NIC0	mgmt-subnet	Management
NIC1	inside-subnet	Gig0/0
NIC2	outside-subnet	Gig0/1

Threat Defense Virtual-3-NICs

Deploy Threat Defense Virtual without Diagnostic Interface on Azure

Perform the steps given below to deploy Threat Defense Virtual without diagnostic interface.

Procedure

Step 1 Depending on your deployment option, you can enable this feature by using one of the methods given below.

- **Solution template in the Azure Marketplace** – On the Azure console, search for **`Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG`** and click **Create**. In the **Basics** window, enter the required information and choose **7.4.x** from the **Software version** drop-down list. Choose the **No** button next to **Attach diagnostic interface**. By default, **No** is selected.

  For the complete procedure to deploy Threat defense virtual on Azure using the solution template in the Azure marketplace, see Deploy from the Azure Marketplace Using the Solution Template.

- **Custom Template using a Managed Image from a VHD** – Go to **Virtual machines** > **+ Create** > **Azure Virtual Machine** > **Advanced** window, and 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 that you can enter in the **Custom data** field 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 **Customdata** field in the ARM template that is used for fresh deployment. By default, the key-value pair is set to **`Diagnostic: ON`** and the diagnostic interface comes up. When the key-value pair is set to **`Diagnostic: OFF`**, the deployment comes up without the diagnostic interface.

For the complete procedure to deploy Threat defense virtual on Azure with a custom template using a managed image from VHD, see Deploy from Azure Using a VHD and Resource Template.

Step 2 Attach the required minimum number of NICs - 3. For more information on attaching interfaces on Azure, see Add network interfaces to or remove network interfaces from virtual machines on Azure.

Figure 1: Network Interface Attachment on Azure

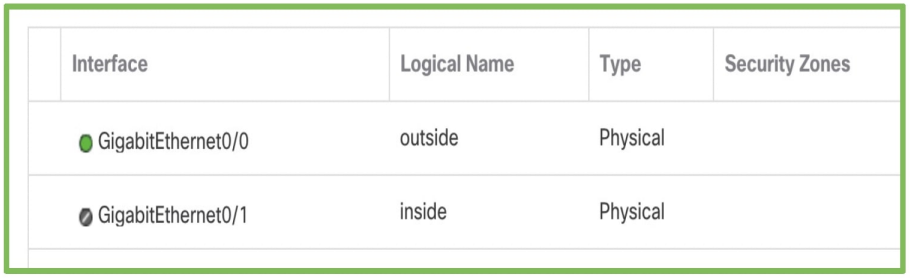
For more information on interfaces, see Interface Overview.

Step 3 (Optional) Use the **show interface ip brief** command on the console to display interface details. You can also view interface details on the Management Center Virtual as given below

The interfaces are displayed on the Management Center Virtual as given below.

Interface	Logical Name	Type	Security Zones
Management0/0	management	Physical	
GigabitEthernet0/0		Physical	
GigabitEthernet0/1		Physical	

With Diagnostic Interface



Interface	Logical Name	Type	Security Zones
GigabitEthernet0/0	outside	Physical	
GigabitEthernet0/1	inside	Physical	

Without Diagnostic Interface

Upgrade Scenarios

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

- All Secure firewall versions – You can upgrade a Threat Defense Virtual instance deployed with a diagnostic interface to a Threat Defense Virtual instance with a diagnostic interface.
- Secure Firewall version 7.4 and later – You can upgrade a Threat Defense Virtual instance deployed without a diagnostic interface to a Threat Defense Virtual instance without a diagnostic interface.

The upgrade scenarios given below are not supported.

- All Secure firewall versions – You cannot upgrade a Threat Defense Virtual instance deployed with a diagnostic interface to a Threat Defense Virtual instance without a diagnostic interface.
- Secure Firewall version 7.4.1 and later – You cannot upgrade a Threat Defense Virtual instance deployed without a diagnostic interface to a Threat Defense Virtual instance with 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 without Diagnostic Interface

To perform a new deployment of a Threat Defense Virtual cluster or an auto scale solution consisting of Threat Defense Virtual instances without the diagnostic interface, ensure that the key-value pair, **Diagnostic: OFF/ON**, is set to **OFF** in the day-0 configuration script.

Troubleshooting

If the diagnostic interface is not removed when the Threat Defense Virtual is deployed, check if the key-value pair, **Diagnostic: OFF/ON**, has been set to **OFF** in the day-0 configuration script.

Auto Scale Solution for the Threat Defense Virtual on Azure

Overview

The auto scale solution enables allocation of resources to match performance requirements and reduce costs. If the demand for resources increases, the system ensures that resources are allocated as required. If the demand for resources decreases, resources are deallocated to reduce costs.

The threat defense virtual auto scale for Azure is a complete serverless implementation which makes use of serverless infrastructure provided by Azure (Logic App, Azure Functions, Load Balancers, Security Groups, Virtual Machine Scale Set, etc.).

Some of the key features of the threat defense virtual auto scale for Azure implementation include:

- Azure Resource Manager (ARM) template-based deployment.
- Support for scaling metrics based on CPU and memory (RAM).

Note See Auto Scale Logic, on page 60 for more information.

- Support for threat defense virtual deployment and multi-availability zones.
- Completely automated threat defense virtual instance registration and de-registration with the management center.
- NAT policy, Access Policy, and Routes automatically applied to scaled-out threat defense virtual instances.
- Support for Load Balancers and multi-availability zones.
- Support for enabling and disabling the auto scale feature.
- Works only with the management center; the device manager is not supported.

- Support to deploy the threat defense virtual with PAYG or BYOL licensing mode. PAYG is applicable only for threat defense virtual software version 6.5 and onwards. See Supported Software Platforms, on page 24.
- Cisco provides an auto scale for Azure deployment package to facilitate the deployment.

The threat defense virtual auto scale solution on Azure supports two types of use cases configured using different topologies:

- Auto scale using Sandwich Topology – The threat defense virtual scale set is sandwiched between an Azure Internal load balancer (ILB) and an Azure External load balancer (ELB).
- Auto scale with Azure Gateway load balancer (GWLB) – The Azure GWLB is integrated with Secure Firewall, public load balancer, and internal servers - to simplify deployment, management, and scaling of firewalls.

Supported Software Platforms

The threat defense virtual auto scale solution is applicable to the threat defense virtual managed by the management center, and is software version agnostic. The Cisco Secure Firewall Threat Defense Compatibility Guide provides software and hardware compatibility, including operating system and hosting environment requirements.

- The Management Centers: Virtual table lists compatibility and virtual hosting environment requirements for the management center virtual.
- The Threat Defense Virtual Compatibility table lists compatibility and virtual hosting environment requirements for the threat defense virtual on Azure.

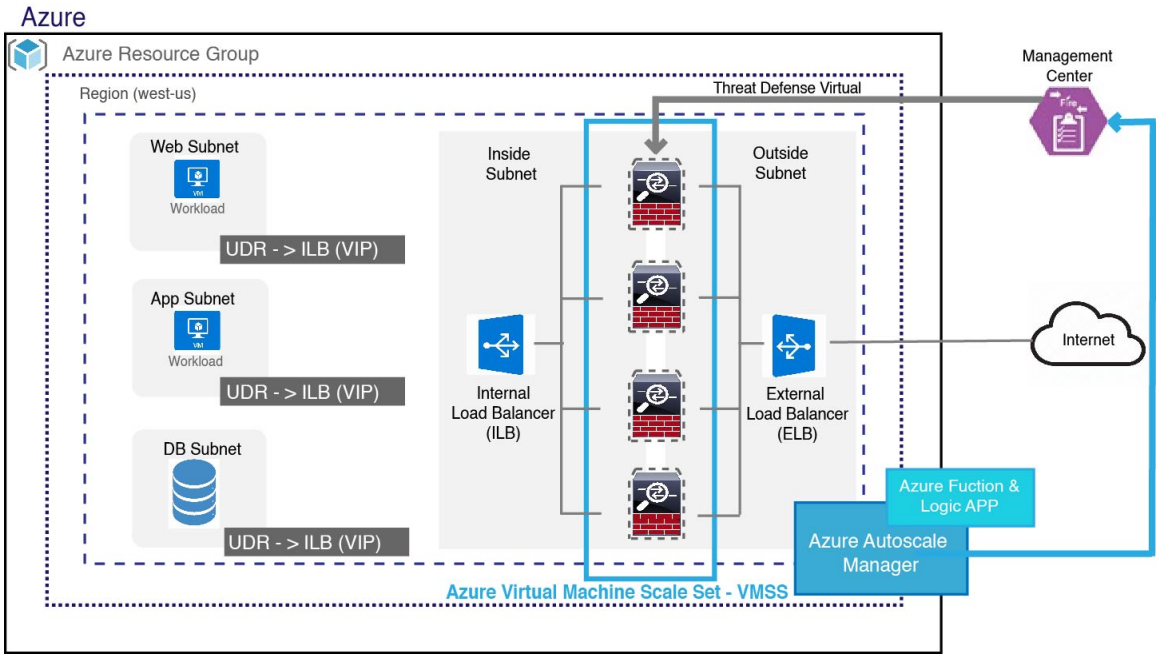
Note For purposes of deploying the Azure auto scale solution, the minimum supported version for the threat defense virtual on Azure is Version 6.4.

Auto Scale using Sandwich Topology Use Case

The threat defense virtual auto scale for Azure is an automated horizontal scaling solution that positions the threat defense virtual scale set sandwiched between an Azure Internal load balancer (ILB) and an Azure External load balancer (ELB).

- The ELB distributes traffic from the Internet to threat defense virtual instances in the scale set; the firewall then forwards traffic to application.
- The ILB distributes outbound Internet traffic from an application to threat defense virtual instances in the scale set; the firewall then forwards traffic to Internet.
- A network packet will never pass through both (internal & external) load balancers in a single connection.
- The number of threat defense virtual instances in the scale set will be scaled and configured automatically based on load conditions.

Figure 2: Threat Defense Virtual Auto Scale using Sandwich Topology Use Case Diagram



Auto Scale with Azure Gateway Load Balancer Use Case

The Azure Gateway Load Balancer (GWLB) ensures that internet traffic to and from an Azure VM, such as an application server, is inspected by Secure Firewall without requiring any routing changes. This integration of the Azure GWLB with Secure Firewall simplifies deployment, management, and scaling of firewalls. This integration also reduces operational complexity and provides a single entry and exit point for traffic at the firewall. The applications and infrastructure can maintain visibility of source IP address, which is critical in some environments.

In the Azure GWLB Auto Scale use case, the threat defense virtual uses only two interfaces: Management and one data interface.

Note

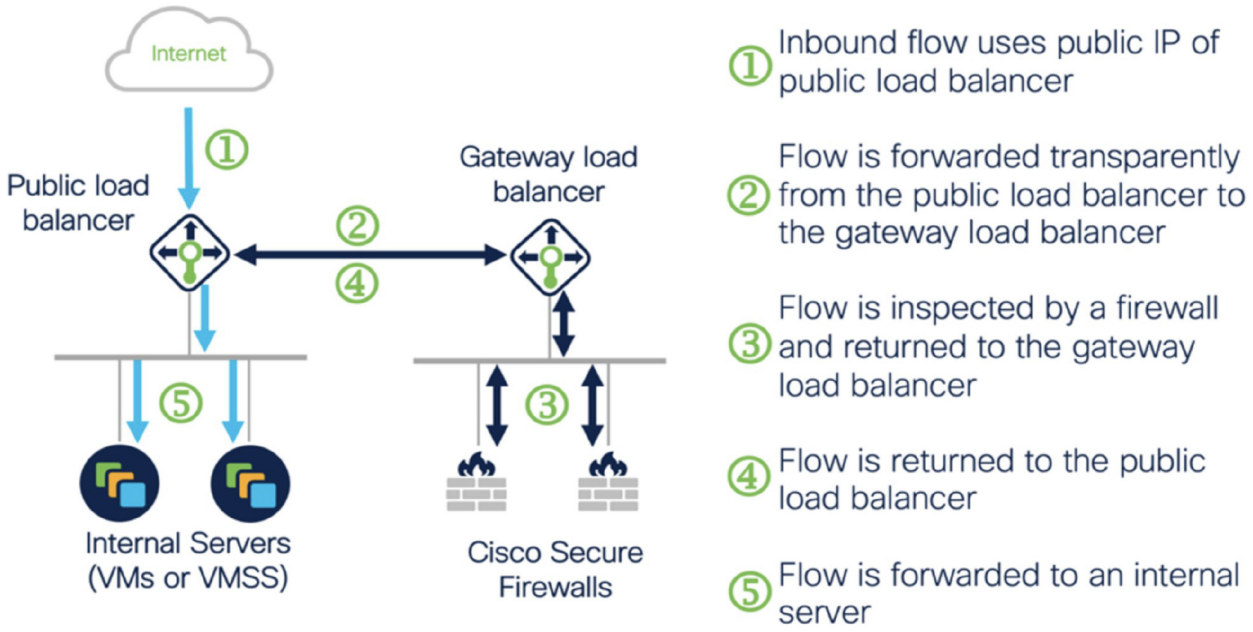
- Network Address Translation (NAT) is not required if you are deploying the Azure GWLB.
- Only IPv4 is supported.

Licensing

Both PAYG and BYOL are supported.

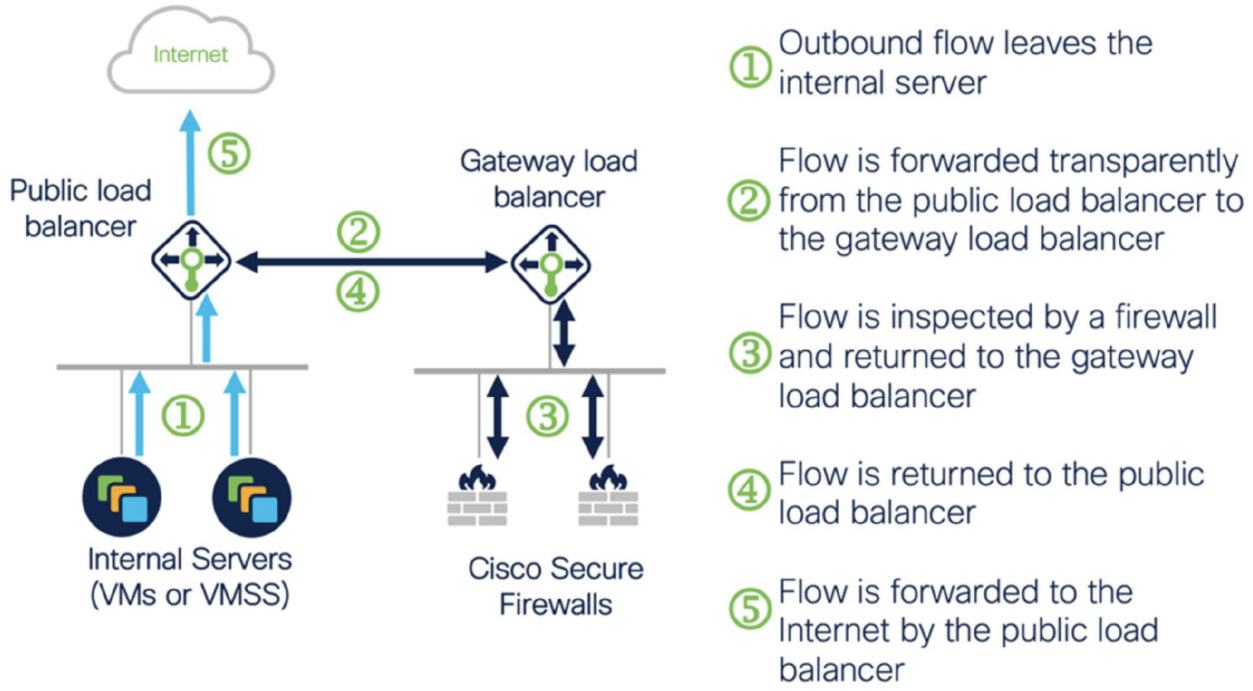
Inbound Traffic Use Case and Topology

The following diagram displays the traffic flow for inbound traffic.



Outbound Traffic Use Case and Topology

The following diagram displays the traffic flow for outbound traffic.

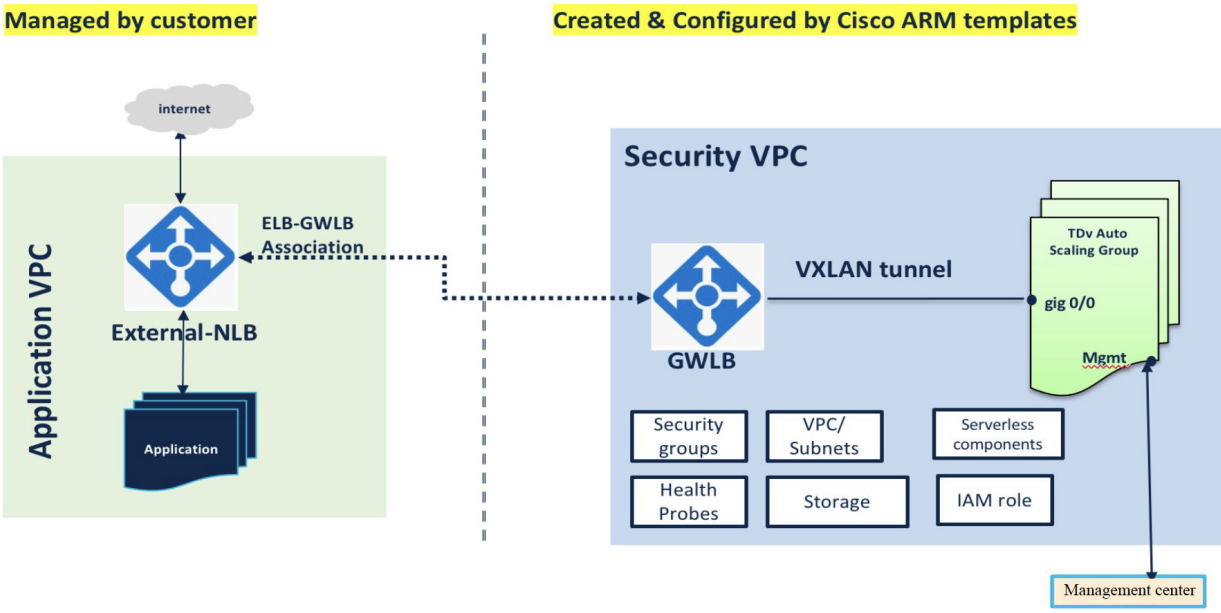


Note To deploy and configure the management center, see the procedures in the Cisco Secure Firewall Management Center Device Configuration Guide. Use the deployed management center to manage the threat defense virtual instances.

Traffic Flow between the Application VPC and Security VPC

In the diagram shown below, traffic is redirected from the existing topology to the firewalls for inspection by the external load balancer. The traffic is then routed to the newly created GWLB. Any traffic that is routed to the ELB is forwarded to the GWLB.

The GWLB then forwards the VXLAN-encapsulated traffic to a threat defense virtual instance. You have to create two threat defense virtual associations as the GWLB uses two separate VXLAN tunnels for ingress and egress traffic. The threat defense virtual decapsulates the VXLAN-encapsulated traffic, inspects it, and routes the traffic to the GWLB. The GWLB then forwards the traffic to the ELB.



Scope

This document covers the detailed procedures to deploy the serverless components for the threat defense virtual auto scale for Azure solution and the auto scale with Azure GWLB solution.

Important

- Read the entire document before you begin your deployment.
- Make sure the prerequisites are met before you start deployment.
- Make sure you follow the steps and order of execution as described herein.

Download the Deployment Package

The threat defense virtual auto scale for Azure solution using sandwich topology is an Azure Resource Manager (ARM) template-based deployment which makes use of the serverless infrastructure provided by Azure (Logic App, Azure Functions, Load Balancers, Virtual Machine Scale Set, and so on).

The threat defense virtual auto scale with Azure GWLB solution is an ARM template-based deployment that creates the GWLB, networking infrastructure, threat defense virtual auto scaling group, serverless components, and other required resources.

The deployment procedure for both the solutions are similar.

Download the files required to launch the threat defense virtual auto scale for Azure solution. Deployment scripts and templates for your version are available in the GitHub repository.

Attention Note that Cisco-provided deployment scripts and templates for auto scale are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

See Build Azure Functions from Source Code, on page 63 for instructions on how to build the *ASM_Function.zip* package.

Auto Scale Solution Components

The following components make up the threat defense virtual auto scale for Azure solution.

Azure Functions (Function App)

The Function App is a set of Azure functions. The basic functionality includes:

- Communicate/Probe Azure metrics periodically.
- Monitor the threat defense virtual load and trigger Scale In/Scale Out operations.
- Register a new threat defense virtual with the management center.
- Configure a new threat defense virtual via management center.
- Unregister (remove) a scaled-in threat defense virtual from the management center.

These functions are delivered in the form of compressed Zip package (see Build the Azure Function App Package, on page 31). The functions are as discrete as possible to carry out specific tasks, and can be upgraded as needed for enhancements and new release support.

Orchestrator (Logic App)

The Auto Scale Logic App is a workflow, i.e. a collection of steps in a sequence. Azure functions are independent entities and cannot communicate with each other. This orchestrator sequences the execution of these functions and exchanges information between them.

- The Logic App is used to orchestrate and pass information between the auto scale Azure functions.
- Each step represents an auto scale Azure function or built-in standard logic.

- The Logic App is delivered as a JSON file.
- The Logic App can be customized via the GUI or JSON file.

Virtual Machine Scale Set (VMSS)

The VMSS is a collection of homogeneous virtual machines, such as threat defense virtual devices.

- The VMSS is capable of adding new identical VMs to the set.
- New VMs added to the VMSS are automatically attached with Load Balancers, Security Groups, and network interfaces.
- The VMSS has a built–in auto scale feature which is disabled for threat defense virtual for Azure.
- You should not add or delete threat defense virtual instances in the VMSS manually.

Azure Resource Manager (ARM) Template

ARM templates are used to deploy the resources required by the threat defense virtual auto scale for Azure solution.

Threat defense virtual auto scale for Azure - The ARM template **azure_ftdv_autoscale.json** provides input for the Auto Scale Manager components including:

- Azure Function App
- Azure Logic App
- The Virtual Machine Scale Set (VMSS)
- Internal/External load balancers.
- Security Groups and other miscellaneous components needed for deployment.

Threat defense virtual auto scale with Azure GWLB - The ARM template **azure_ftdv_autoscale_with_GWLB.json** provides input for the Auto Scale Manager components including:

- Azure Function App
- Azure Logic App
- Virtual Machine (VM) or Virtual Machine Scale Set (VMSS)
- Networking Infrastructure
- Gateway load balancer
- Security Groups and other miscellaneous components needed for deployment

Important The ARM template has limitations with respect to validating user input, hence it is your responsibility to validate input during deployment.

Prerequisites

Azure Resources

Resource Group

An existing or newly created Resource Group is required to deploy all the components of this solution.

Note Record the Resource Group name, the Region in which it is created, and the Azure Subscription ID for later use.

Networking

Make sure a virtual network is available or created. An auto scale deployment with sandwich topology does not create, alter, or manage any networking resources. However, note that auto scale deployment with the Azure GWLB creates networking infrastructure.

The threat defense virtual requires four network interfaces, thus your virtual network requires four subnets for:

1. Management traffic
2. Diagnostic traffic
3. Inside traffic
4. Outside traffic

The following ports should be open in the Network Security Group to which the subnets are connected:

- SSH(TCP/22)

  Required for the Health probe between the Load Balancer and threat defense virtual.

  Required for communication between the Serverless functions and threat defense virtual.

- TCP/8305

  Required for communication between threat defense virtual and the management center.

- HTTPS(TCP/443)

  Required for communication between the Serverless components and the management center.

- Application-specific protocol/ports

  Required for any user applications (for example, TCP/80, etc.).

Note Record the virtual network name, the virtual network CIDR, the names of the 4 subnets, and the Gateway IP addresses of the outside and inside subnets.

Build the Azure Function App Package

The threat defense virtual auto scale solution requires that you build an archive file: *ASM_Function.zip*. which delivers a set of discrete Azure functions in the form of a compressed ZIP package.

See Build Azure Functions from Source Code, on page 63 for instructions on how to build the *ASM_Function.zip* package.

These functions are as discrete as possible to carry out specific tasks, and can be upgraded as needed for enhancements and new release support.

Prepare the Management Center

You manage the threat defense virtual using the management center, a full-featured, multidevice manager. The threat defense virtual registers and communicates with the management center on the Management interface that you allocated to the threat defense virtual machine.

Create all the objects needed for the threat defense virtual configuration and management, including a device group, so you can easily deploy policies and install updates on multiple devices. All the configurations applied on the device group will be pushed to the threat defense virtual instances.

The following sections provide a brief overview of basic steps to prepare the management center. You should consult the full Secure Firewall Management Center Configuration Guide for complete information. When you prepare the management center, make sure you record the following information:

- The management center public IP address.
- The management center username/password.
- The security policy name.
- The inside and outside security zone object names.
- The device group name.

Create a New Management Center User

Create a new user in the management center with Admin privileges to be used only by AutoScale Manager.

Important It's important to have the management center user account dedicated to the threat defense virtual auto scale solution to prevent conflicts with other management center sessions.

Procedure

Step 1 Create new user in the management center with Admin privileges. Choose **System** > **Users** and click **Create User**.

The username must be Linux-valid:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Step 2 Complete user options as required for your environment. See the Cisco Secure Firewall Management Center Administration Guide for complete information.

Configure Access Control

Configure access control to allow traffic from inside to outside. Within an access control policy, access control rules provide a granular method of handling network traffic across multiple managed devices. Properly configuring and ordering rules is essential to building an effective deployment. See "Best Practices for Access Control" in the Cisco Secure Firewall Management Center Device Configuration Guide.

Procedure

Step 1 Choose **Policies** > **Access Control**.

Step 2 Click **New Policy**.

Step 3 Enter a unique **Name** and, optionally, a **Description**.

Step 4 See the Cisco Secure Firewall Management Center Device Configuration Guide to configure security settings and rules for your deployment.

Configure Licensing

All licenses are supplied to the threat defense by the management center. You can optionally purchase the following feature licenses:

- **Secure Firewall Threat Defense IPS**—Security Intelligence and Cisco Secure IPS
- **Secure Firewall Threat Defense Malware Defense**—Malware Defense
- **Secure Firewall Threat Defense URL Filtering**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

Note When you buy a IPS , malware defense, or URL filtering license, you also need a matching subscription license to access updates for 1, 3, or 5 years.

Before you begin

- Have a master account on the Cisco Smart Software Manager.

  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

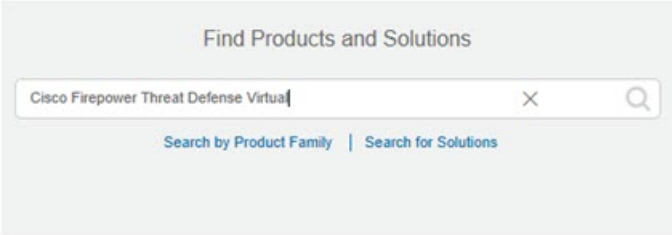
- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the Cisco Commerce Workspace. Search for the following license PIDs:

Figure 3: License Search



Note
If a PID is not found, you can add the PID manually to your order.

Step 2 If you have not already done so, register the management center with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the Cisco Secure Firewall Management Center Administration Guide for detailed instructions.

Create Security Zone Objects

Create inside and outside security zone objects for your deployment.

Procedure

Step 1 Choose **Objects** > **Object Management**.
Step 2 Choose **Interface** from the list of object types.
Step 3 Click **Add** > **Security Zone**.
Step 4 Enter a **Name** (for example *inside*, *outside*).
Step 5 Choose **Routed** as the **Interface Type**.
Step 6 Click **Save**.

Create a Device Group

Device groups enable you to easily assign policies and install updates on multiple devices.

Procedure

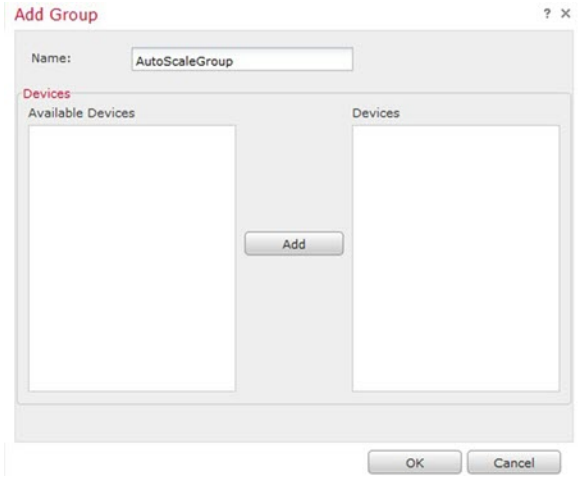
Step 1 Choose **Devices** > **Device Management**.

Figure 4: Device Management

Step 2 From the **Add** drop-down menu, choose **Add Group**.

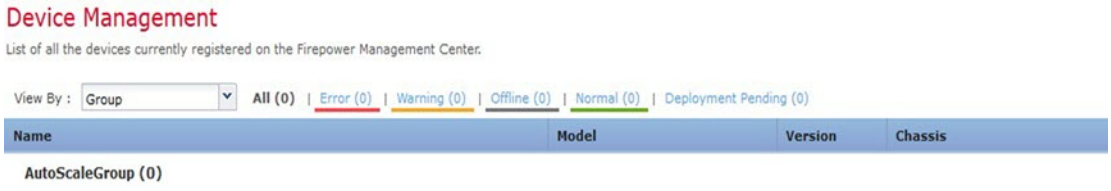
Step 3 Enter a **Name**. For example, *AutoScaleGroup*.

Figure 5: Add Device Group



Step 4 Click **OK** to add the device group.

Figure 6: Device Group Added



Configure Secure Shell Access

Platform settings for threat defense devices configure a range of unrelated features whose values you might want to share among several devices. Threat Defense Virtual Auto Scale for Azure requires a threat defense Platform Settings Policy to allow SSH on the Inside/Outside zones and the device group created for the auto scale Group. This is required so that the threat defense virtual's data interfaces can respond to Health Probes from Load Balancers.

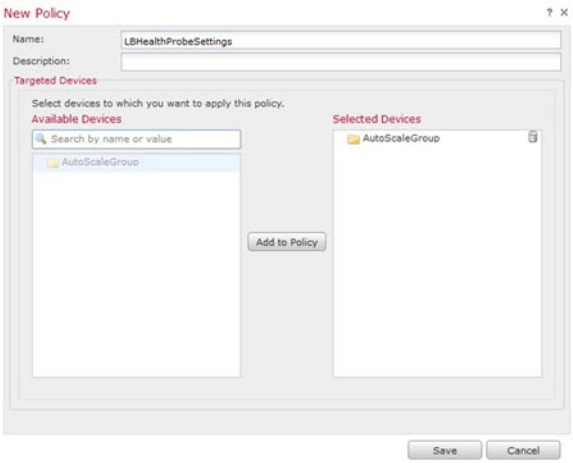
Before you begin

You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects. For example, see the *azure-utility-ip (168.63.129.16)* object in the following procedure.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a threat defense policy, for example *LBHealthProbeSettings*.

Figure 7: Threat Defense Platform Settings Policy



Step 2 Select **Secure Shell**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

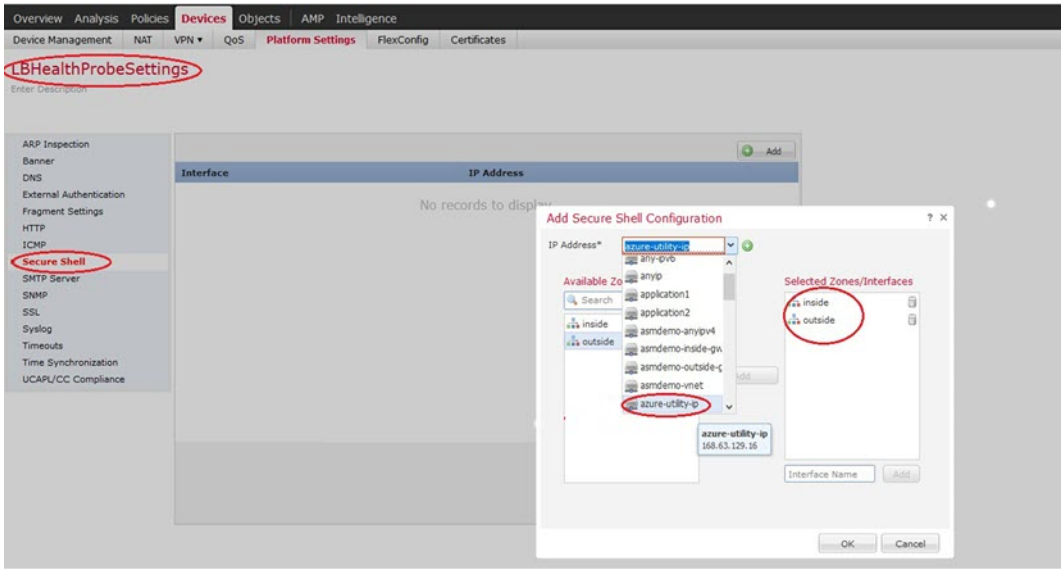
- **IP Address**—The network object that identifies the hosts or networks you are allowing to make SSH connections (for example, *azure-utility-ip (168.63.129.16)*). Choose an object from the drop-down menu, or add a new network object by clicking +.
- **Security Zones**—Add the zones that contain the interfaces to which you will allow SSH connections. For example, you can assign the inside interface to the **inside** zone; and the outside interface to the **outside** zone. You can create security zones from the management center's **Objects** page. See the Cisco Secure Firewall Management Center Device Configuration Guide for complete information about security zones.

Note

Inside interfaces are not used in the Auto Scale with Azure Gateway Load Balancer use case.

- Click **OK**.

Figure 8: SSH Access for the Threat Defense Virtual Auto Scale



Step 4 Click **Save**.

You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Note
You can also configure TCP port 443 for the health probe instead of using **SSH Access**. To do this, go to **Devices > Platform settings > HTTP Access**, select the **Enable HTTP Server** checkbox, and enter **443** in the **Port** field. Associate this setting with the inside and outside interfaces. You have to also change the health probe port in the ARM template to 443. For more information on configuring HTTP Access, see Configuring HTTP.

Configure NAT

Create a NAT policy and create the necessary NAT rules to forward traffic from the outside interface to your application, and attach this policy to the device group you created for auto scale.

Note You have to configure NAT only if you are configuring auto scale using a sandwich topology.

Procedure

Step 1 Choose **Devices** > **NAT**.

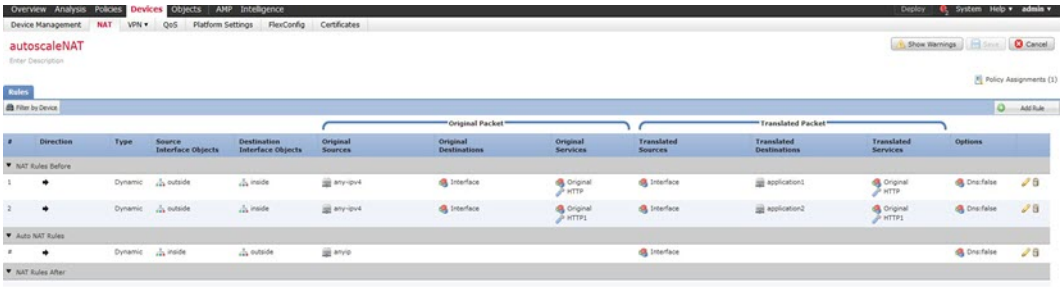
Step 2 From the **New Policy** drop-down list, choose **Threat Defense NAT**.

Step 3 Enter a unique **Name**.

Step 4 Optionally, enter a **Description**.

Step 5 Configure your NAT rules. See the procedure "Configure NAT for Threat Defense" in the Cisco Secure Firewall Management Center Device Configuration Guide for guidelines on how to create NAT rules and apply NAT policies. The following figure shows a basic approach.

Figure 9: NAT Policy Example



Note
We recommend that you keep your rules as simple as possible to avoid translation problems and difficult troubleshooting situations. Careful planning before you implement NAT is critical.

Step 6 Click **Save**.

Input Parameters

The following table defines the template parameters and provides an example. Once you decide on these values, you can use these parameters to create the threat defense virtual device when you deploy the ARM template into your Azure subscription. See Deploy the Auto Scale ARM Template, on page 44.In the Auto scale with Azure GWLB solution, networking infrastructure is also created due to which additional input parameters have to be configured in the template. The parameter descriptions are self-explanatory.

Table 2: Template Parameters

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
resourceNamePrefix	String* (3-10 characters)	All the resources are created with name containing this prefix. Note: Use only lowercase letters. Example: ftdv	New
virtualNetworkRg	String	The virtual network resource group name. Example: cisco-virtualnet-rg	Existing

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
virtualNetworkName	String	The virtual network name (already created). Example: cisco-virtualnet	Existing
virtualNetworkCidr	CIDR format x.x.x.x/y	CIDR of Virtual Network (already created)	Existing
mgmtSubnet	String	The management subnet name (already created). Example: cisco-mgmt-subnet	Existing
diagSubnet	String	The diagnostic subnet name (already created). Example: cisco-diag-subnet	Existing
insideSubnet	String	The inside Subnet name (already created). Example: cisco-inside-subnet	Existing
internalLbIp	String	The internal load balancer IP address for the inside subnet (already created). Example: 1.2.3.4	Existing
insideNetworkGatewayIp	String	The inside subnet gateway IP address (already created).	Existing
outsideSubnet	String	The outside subnet name (already created). Example: cisco-outside-subnet	Existing
outsideNetworkGatewayIp	String	The outside subnet gateway IP (already created).	Existing
deviceGroupName	String	Device group in management center (already created)	Existing
insideZoneName	String	Inside Zone name in the management center (already created)	Existing
outsideZoneName	String	Outside Zone name in the management center (already created)	Existing

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
softwareVersion	String	The threat defense virtual Version (selected from drop-down during deployment).	Existing
vmSize	String	Size of threat defense virtual instance (selected from drop-down during deployment).	N/A
ftdLicensingSku	String	Threat Defense Virtual Licensing Mode (PAYG/BYOL) Note: PAYG is supported in Version 6.5+.	N/A
licenseCapability	Comma-separated string	BASE, MALWARE, URLFilter, THREAT	N/A
ftdVmManagementUserName	String*	The threat defense virtual VM management administrator user name. This **cannot** be 'admin'. See Azure for VM administrator user name guidelines.	New
ftdVmManagementUserPassword	String*	Password for the threat defense virtual VM management administrator user. Passwords must be 12 to 72 characters long, and must have: lowercase, uppercase, numbers, and special characters; and must have no more than 2 repeating characters. **Note** There is no compliance check for this in the template.	New
fmcIpAddress	String x.x.x.x	The public IP address of the management center (already created)	Existing
fmcUserName	String	Management Center user name, with administrative privileges (already created)	Existing
fmcPassword	String	Management Center password for above management center user name (already created)	Existing

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
policyName	String	Security Policy created in the management center (already created)	Existing
scalingPolicy	POLICY-1 / POLICY-2	**POLICY-1**: Scale-Out will be triggered when the average load of any threat defense virtual goes beyond the Scale Out threshold for the configured duration. **POLICY-2**: Scale-Out will be triggered when average load of all the threat defense virtual devices in the auto scale group goes beyond the Scale Out threshold for the configured duration. In both cases Scale-In logic remains the same: Scale-In will be triggered when average load of all the threat defense virtual devices comes below the Scale In threshold for the configured duration.	N/A
scalingMetricsList	String	Metrics used in making the scaling decision. Allowed: CPU CPU, MEMORY Default: CPU	N/A
cpuScaleInThreshold	String	The Scale-In threshold in percent for CPU metrics. Default: 10 When the threat defense virtual metric goes below this value the Scale-In will be triggered. See Auto Scale Logic, on page 60.	N/A

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
cpuScaleOutThreshold	String	The Scale-Out threshold in percent for CPU metrics. Default: 80 When the threat defense virtual metric goes above this value, the Scale-Out will be triggered. The 'cpuScaleOutThreshold' should always be **greater** than the 'cpuScaleInThreshold'. See Auto Scale Logic, on page 60.	N/A
memoryScaleInThreshold	String	The Scale-In threshold in percent for memory metrics. Default: 0 When the threat defense virtual metric goes below this value the Scale-In will be triggered. See Auto Scale Logic, on page 60.	N/A
memoryScaleOutThreshold	String	The Scale-Out threshold in percent for memory metrics. Default: 0 When the threat defense virtual metric goes above this value, the Scale-Out will be triggered. The 'memoryScaleOutThreshold´ should always be **greater** than the 'memoryScaleInThreshold'. See Auto Scale Logic, on page 60.	N/A
minFtdCount	Integer	The minimum threat defense virtual instances available in the scale set at any given time. Example: 2	N/A

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
maxFtdCount	Integer	The maximum threat defense virtual instances allowed in the Scale set. Example: 10 **Note** This number is restricted by the management center capacity. The Auto Scale logic will not check the range of this variable, hence fill this carefully.	N/A
metricsAverageDuration	Integer	Select from the drop-down. This number represents the time (in minutes) over which the metrics are averaged out. If the value of this variable is 5 (i.e. 5min), when the Auto Scale Manager is scheduled it will check the past 5 minutes average of metrics and based on this it will make a scaling decision. **Note** Only numbers 1, 5, 15, and 30 are valid due to Azure limitations.	N/A

Parameter Name	Allowed Values/Type	Description	Resource Creation Type
initDeploymentMode	BULK / STEP	Primarily applicable for the first deployment, or when the Scale Set does not contain any threat defense virtual instances. BULK: The Auto Scale Manager will try to deploy 'minFtdCount' number of threat defense virtual instances in parallel at one time. **Note** The launch is in parallel, but registering with the management center is sequential due to management center limitations. STEP: The Auto Scale Manager will deploy the 'minFtdCount' number of threat defense virtual devices one by one at each scheduled interval. **Note** The STEP option will take a long time for the ‘minFtdCount’ number of instances to be launched and configured with the management center and become operational, but useful in debugging. The BULK option takes same amount of time to launch all ‘minFtdCount’ number of threat defense virtual as one threat defense virtual launch takes (because it runs in parallel), but the management center registration is sequential. The total time to deploy ‘minFtdCount’ number of threat defense virtual = (time to launch One threat defense virtual + time to register/configure one threat defense virtual * minFtdCount).	
*Azure has restrictions on the naming convention for new resources. Review the limitations or simply use all lowercase. **Do not use spaces or any other special characters**.			

Deploy the Auto Scale Solution

Download the Deployment Package

The threat defense virtual auto scale for Azure solution using sandwich topology is an Azure Resource Manager (ARM) template-based deployment which makes use of the serverless infrastructure provided by Azure (Logic App, Azure Functions, Load Balancers, Virtual Machine Scale Set, and so on).

The threat defense virtual auto scale with Azure GWLB solution is an ARM template-based deployment that creates the GWLB, networking infrastructure, threat defense virtual auto scaling group, serverless components, and other required resources.

The deployment procedure for both the solutions are similar.

Download the files required to launch the threat defense virtual auto scale for Azure solution. Deployment scripts and templates for your version are available in the GitHub repository.

Attention Note that Cisco-provided deployment scripts and templates for auto scale are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

See Build Azure Functions from Source Code, on page 63 for instructions on how to build the *ASM_Function.zip* package.

Deploy the Auto Scale ARM Template

Threat defense virtual auto scale for Azure using Sandwich Topology - Use the ARM template **azure_ftdv_autoscale.json** to deploy the resources required by the threat defense virtual auto scale for Azure. Within a given resource group, the ARM template deployment creates the following:

- Virtual Machine Scale Set (VMSS)
- External Load Balancer
- Internal Load Balancer
- Azure Function App
- Logic App
- Security groups (For Data and Management interfaces)

Threat defense virtual auto scale with Azure GWLB - Use the ARM template **azure_ftdv_autoscale_with_GWLB.json** to deploy the resources required by the threat defense virtual auto scale with Azure GWLB solution. Within a given resource group, the ARM template deployment creates the following:

- Virtual Machine (VM) or Virtual Machine Scale Set (VMSS)
- Gateway Load Balancer
- Azure Function App
- Logic App

- Networking Infrastructure
- Security Groups and other miscellaneous components needed for deployment

Before you begin

- Download the ARM templates from the GitHub repository (https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/azure).

Procedure

Step 1 If you need to deploy the threat defense virtual instances in multiple Azure zones, edit the ARM template based on the zones available in the Deployment region.

Example:

```
"zones": [
    "1",
    "2",
    "3"
],
```

This example shows the “Central US” region which has 3 zones.

Step 2 Edit the traffic rules required in External Load Balancer. You can add any number of rules by extending this ‘json’ array. This is valid for the Auto Scale using Sandwich Topology use case.

Example:

```
{
 "type": "Microsoft.Network/loadBalancers",
 "name": "[variables('elbName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2018-06-01",
 "sku": {
   "name": "Standard"
 },
 "dependsOn": [
   "[concat('Microsoft.Network/publicIPAddresses/', variables('elbPublicIpName'))]"

 ],
 "properties": {
   "frontendIPConfigurations": [
     {
       "name": "LoadBalancerFrontEnd",
         "properties": {
           "publicIPAddress": {
             "id": "[resourceId('Microsoft.Network/publicIPAddresses/',
variables('elbPublicIpName'))]"
           }
         }
     }
   ],
   "backendAddressPools": [
     {
       "name": "backendPool"
```

```
        }
      ],
      "loadBalancingRules": [
        {
          "properties": {
            "frontendIPConfiguration": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/frontendIpConfigurations/LoadBalancerFrontend')]"
            },
            "backendAddressPool": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/backendAddressPools/BackendPool')]"
            },
            "probe": {
            "Id": "[concat(resourceId('Microsoft.Network/loadBalancers', variables('elbName')),
'/probes/lbprobe')]"
            },
            "protocol": "TCP",
            "frontendPort": "80",
            "backendPort": "80",
            "idleTimeoutInMinutes": "[variables('idleTimeoutInMinutes')]"
          },
          "Name": "lbrule"
        }
      ],
```

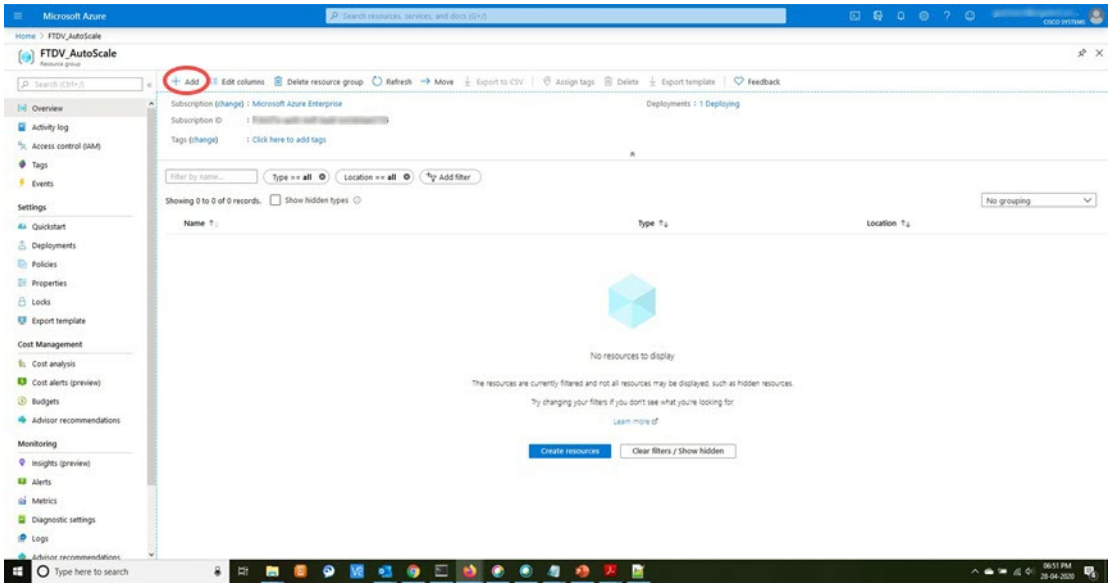
Note
You can also edit this from the Azure portal post-deployment if you prefer not to edit this file.

Step 3 Log in to the Microsoft Azure portal using your Microsoft account username and password.

Step 4 Click **Resource groups** from the menu of services to access the Resource Groups blade. You will see all the resource groups in your subscription listed in the blade.

Create a new resource group or select an existing, empty resource group; for example, *threat defense virtual_AutoScale*.

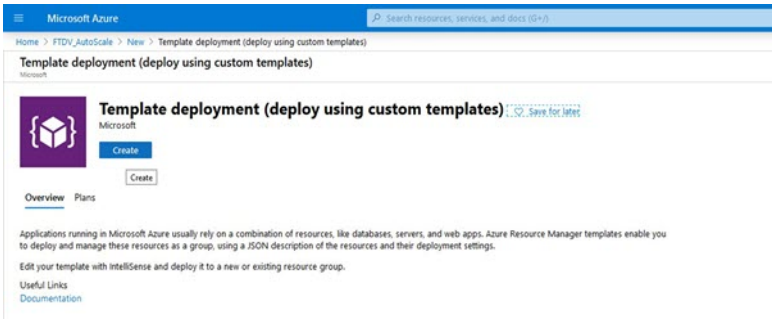
Figure 10: Azure Portal



Step 5 Click **Create a resource (+)** to create a new resource for template deployment. The Create Resource Group blade appears.

Step 6 In **Search the Marketplace**, type **Template deployment (deploy using custom templates)**, and then press **Enter**.

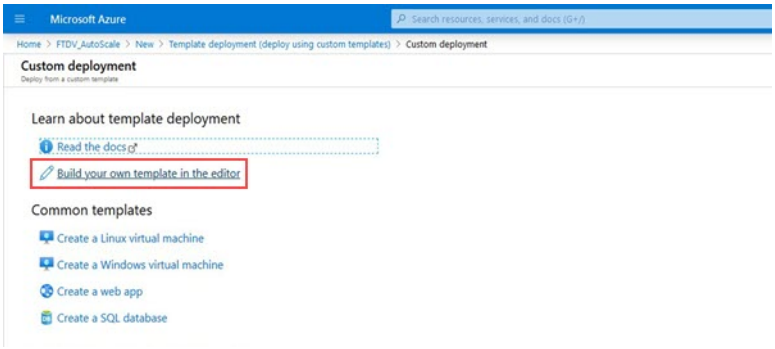
Figure 11: Custom Template Deployment



Step 7 Click **Create**.

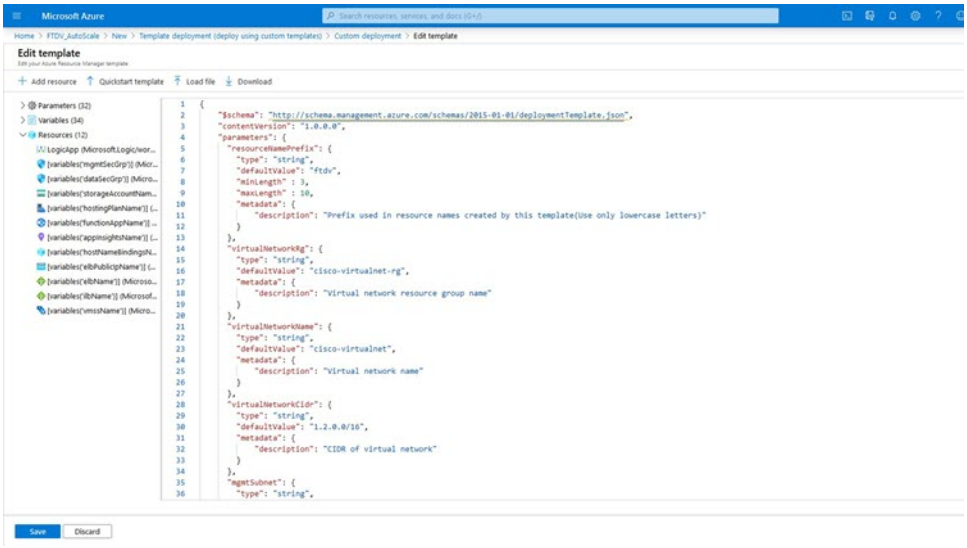
Step 8 There are several options for creating a template. Choose **Build your own template in editor**.

Figure 12: Build Your Own Template



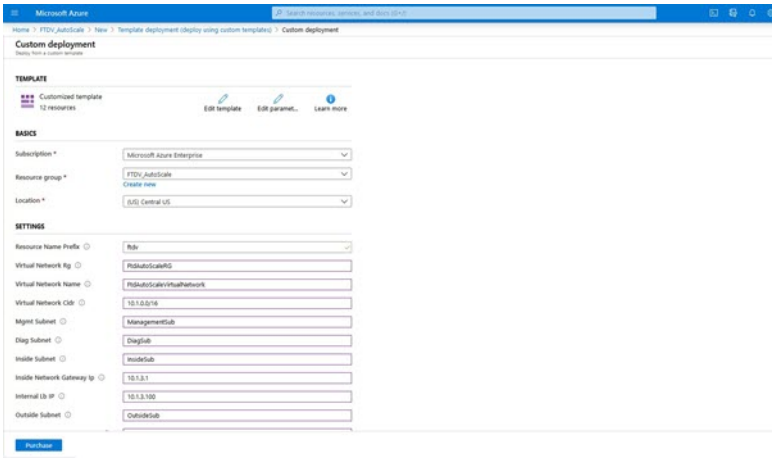
Step 9 In the **Edit template** window, delete all the default content and copy the contents from the updated *azure_ftdv_autoscale.json* and click **Save**.

Figure 13: Edit Template



Step 10 In next section, fill all the parameters. Refer to Input Parameters, on page 37 for details about each parameter, then click **Purchase**.

Figure 14: ARM Template Parameters



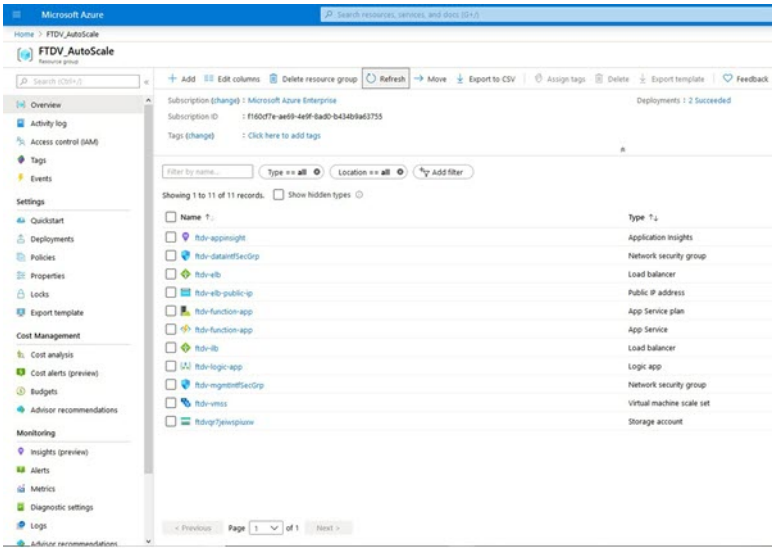
Note

You can also click **Edit Parameters** and edit the JSON file or upload pre-filled contents.

The ARM template has limited input validation capabilities, hence it is your responsibility to validate the input.

Step 11 When a template deployment is successful, it creates all the required resources for the threat defense virtual auto scale for Azure solution. See the resouses in the following figure. The Type column describes each resource, including the Logic App, VMSS, Load Balancers, Public IP address, etc.

Figure 15: Threat Defense Virtual Auto Scale Template Deployment



Deploy the Azure Function App

When you deploy the ARM template, Azure creates a skeleton Function App, which you then need to update and configure manually with the functions required for the Auto Scale Manager logic.

Before you begin

- Build the *ASM_Function.zip* package. See Build Azure Functions from Source Code, on page 63.

Procedure

Step 1 Go to the Function App you created when you deployed the ARM template, and verify that no functions are present. In a browser go to this URL:

https://<Function App Name>.scm.azurewebsites.net/DebugConsole

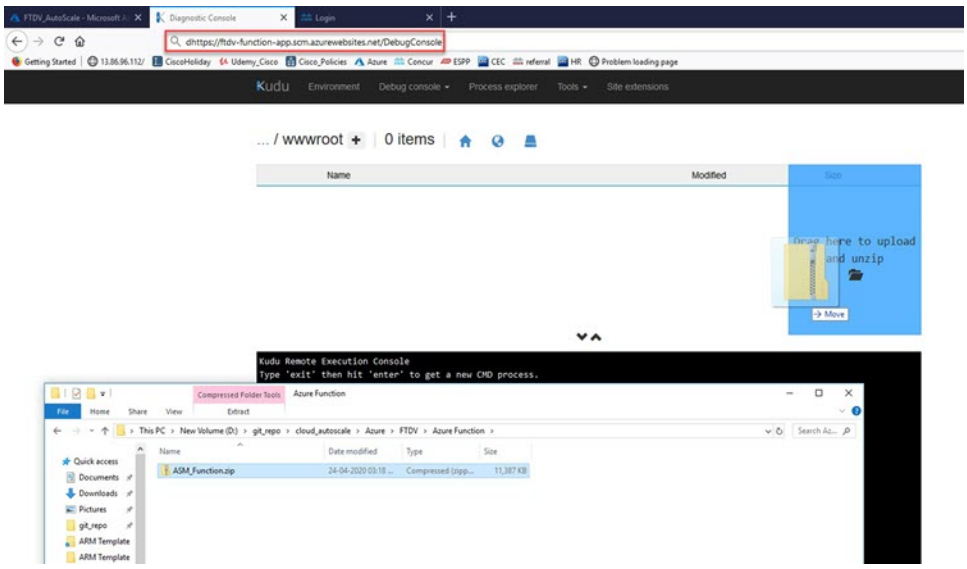
For the example in Deploy the Auto Scale ARM Template, on page 44:

https://ftdv-function-app.scm.azurewebsites.net/DebugConsole

Step 2 In the file explorer navigate to **site/wwwroot**.

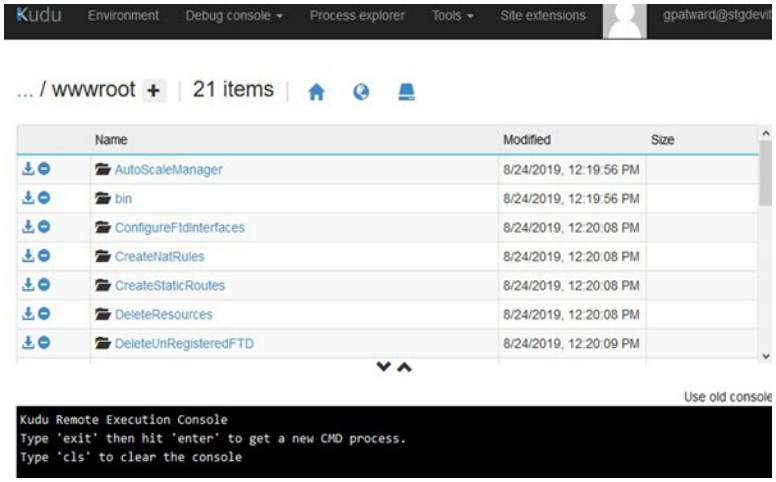
Step 3 Drag-and-drop the **ASM_Function.zip** to the right side corner of the file explorer.

Figure 16: Upload the Threat Defense Virtual Auto Scale Functions



Step 4 Once the upload is successful, all of the serverless functions should appear.

Figure 17: Threat Defense Virtual Serverless Functions

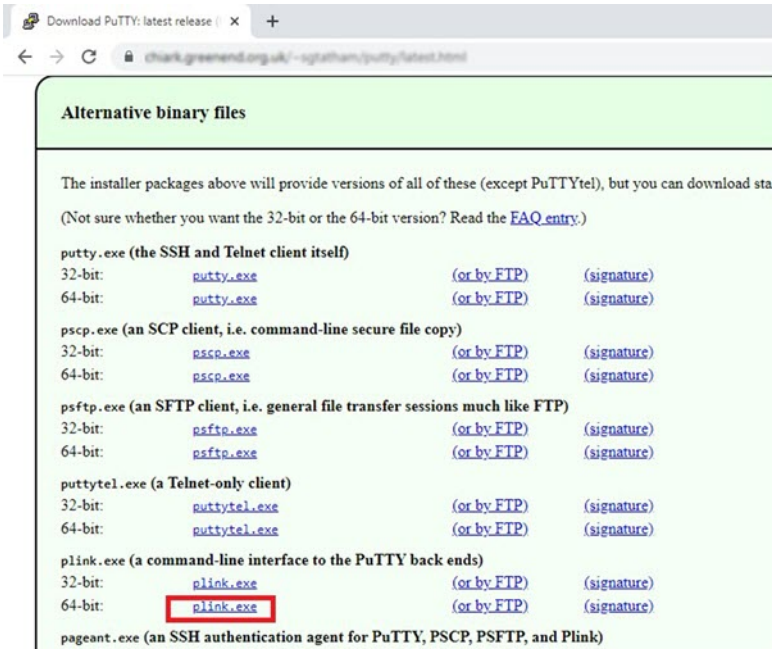


Step 5 Download the PuTTY SSH client.

Azure functions need to access the threat defense virtual via an SSH connection. However, the opensource libraries used in the serverless code do not support the SSH key exchange algorithms used by the threat defense virtual. Hence you need to download a pre-built SSH client.

Download the PuTTY command-line interface to the PuTTY back end (*plink.exe*) from www.putty.org.

Figure 18: Download PuTTY



Step 6 Rename the SSH client executable file **plink.exe** to **ftdssh.exe**.

Step 7 Drag-and-drop the **ftdssh.exe** to the right side corner of the file explorer, to the location where **ASM_Function.zip** was uploaded in the previous step.

Step 8 Verify the SSH client is present with the function application. Refresh the page if necessary.

Fine Tune the Configuration

There are a few configurations available to fine tune the Auto Scale Manager or to use in debugging. These options are not exposed in the ARM template, but you can edit them under the Function App.

Before you begin

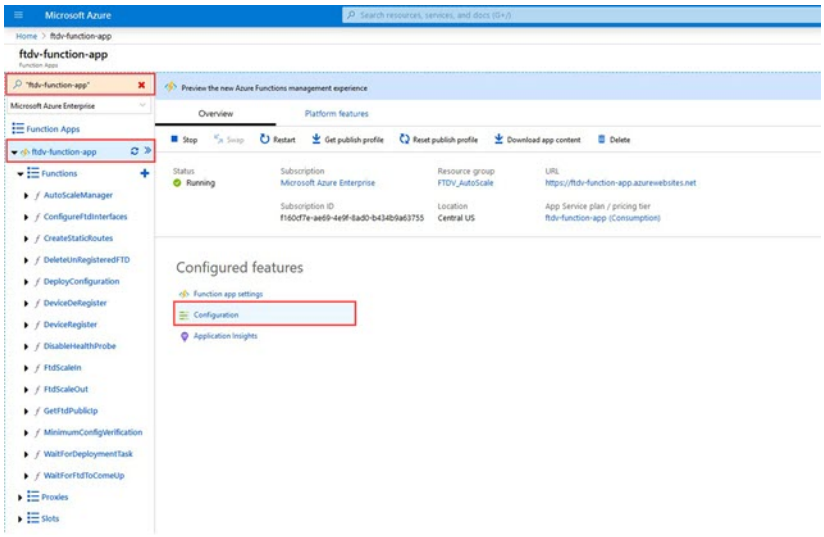
Note This can be edited at any time. Follow this sequence to edit the configurations.

- Disable the Function App.
- Wait for existing scheduled task to finish.
- Edit and save the configuration.
- Enable the Function App.

Procedure

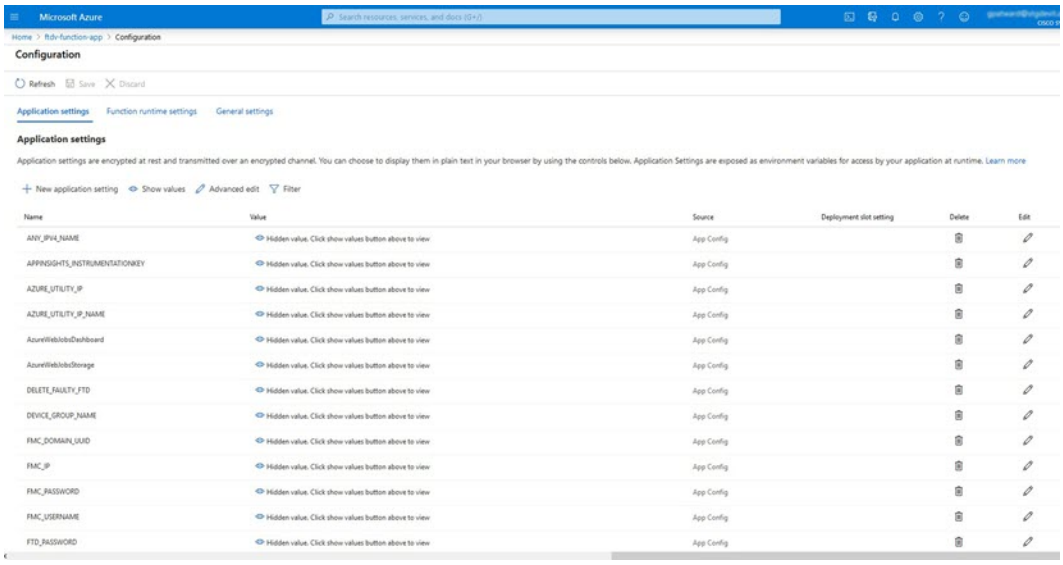
Step 1 In the Azure portal, search for and select the threat defense virtual function application.

Figure 19: Threat Defense Virtual Function Application



Step 2 Configurations passed via the ARM template can also be edited here. Variable names may appear different from the ARM template, but you can easily identify the purpose of these variables from their name.

Figure 20: Application Settings



Most of the options are self-explanatory from the name. For example:

- Configuration Name: “DELETE_FAULTY_FTD” (Default value : YES)

During Scale-Out, a new threat defense virtual instance is launched and registered with the management center. In case the registration fails, based on this option, Auto Scale Manager will decide to keep that threat defense virtual instance or delete it. (YES : Delete faulty threat defense virtual / NO : Keep the threat defense virtual instance even if it fails to register with the management center).

- In the Function App settings, all the variables (including variables containing a secure string like 'password') can be seen in clear text format by users that have access to the Azure subscription.

  If users have any security concerns with this (for example, if an Azure subscription is shared among users with lower privilages within the organization), a user can make use of Azure's *Key Vault* service to protect passwords. Once this is configured, instead of providing a clear text 'password' in function settings, a user has to provide a secure identifier generated by the key vault where the password is stored.

  Note
  Search the Azure documentation to find the best practices to secure your application data.

Configure the IAM Role in the Virtual Machine Scale Set

Azure Identity and Access Management (IAM) is used as a part of Azure Security and Access Control to manage and control a user's identity. Managed identities for Azure resources provides Azure services with an automatically managed identity in Azure Active Directory.

This allows the Function App to control the Virtual Machine Scale Sets (VMSS) without explicit authentication credentials.

Procedure

Step 1 In the Azure portal, go to the VMSS.

Step 2 Click **Access control (IAM)**.

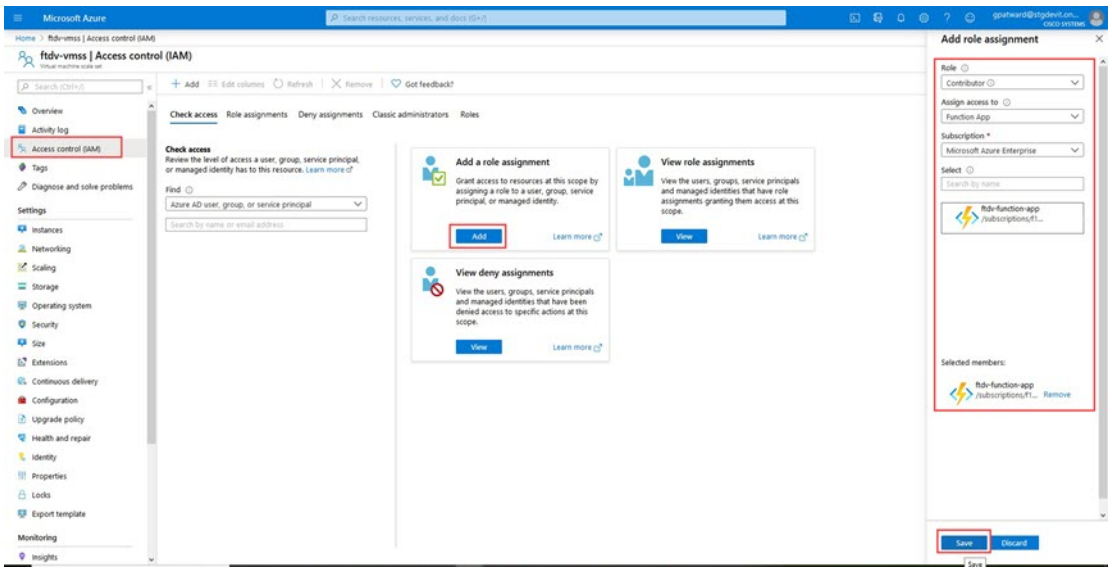
Step 3 Click **Add** to add a role assignment

Step 4 From the **Add role assignment** drop-down, choose **Contributor**.

Step 5 From the **Assign access to** drop-down, choose **Function App**.

Step 6 Select the threat defense virtual function application.

Figure 21: AIM Role Assignment



Step 7 Click **Save**.

Note
You should also verify that there are no threat defense virtual instances launched yet.

Update Security Groups

The ARM template creates two security groups, one for the Management interface, and one for data interfaces. The Management security group will allow only traffic required for threat defense virtual management activities. However, the data interface security group will allow all traffic.

Procedure

Fine tune the security group rules based on the topology and application needs of your deployments.

Note
The data interface security group should allow, at a minimum, SSH traffic from the load balancers.

Update the Azure Logic App

The Logic App acts as the orchestrator for the Autoscale functionality. The ARM template creates a skeleton Logic App, which you then need to update manually to provide the information necessary to function as the auto scale orchestrator.

Procedure

Step 1 From the repository, retrieve the file *LogicApp.txt* to the local system and edit as shown below.

Important
Read and understand all of these steps before proceeding.

These manual steps are not automated in the ARM template so that only the Logic App can be upgraded independently later in time.

a) Required: Find and replace all the occurrences of "SUBSCRIPTION_ID" with your subscription ID information.
b) Required: Find and replace all the occurrences of "RG_NAME" with your resource group name.
c) Required: Find and replace all of the occurrences of "FUNCTIONAPPNAME" to your function app name.

The following example shows a few of these lines in the *LogicApp.txt* file:

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_FTD": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) (Optional) Edit the trigger interval, or leave the default value (5). This is the time interval at which the Autoscale functionality is periodically triggered. The following example shows these lines in the *LogicApp.txt* file:

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
```

```
            "interval": 5
        },
```

e) (Optional) Edit the time to drain, or leave the default value (5). This is the time interval to drain existing connections from the threat defense virtual before deleting the device during the Scale-In operation. The following example shows these lines in the *LogicApp.txt* file:

```
"actions": {
     "Branch_based_on_Scale-In_or_Scale-Out_condition": {
         "actions": {
             "Delay_For_connection_Draining": {
                 "inputs": {
                     "interval": {
                         "count": 5,
                         "unit": "Minute"
                     }
```

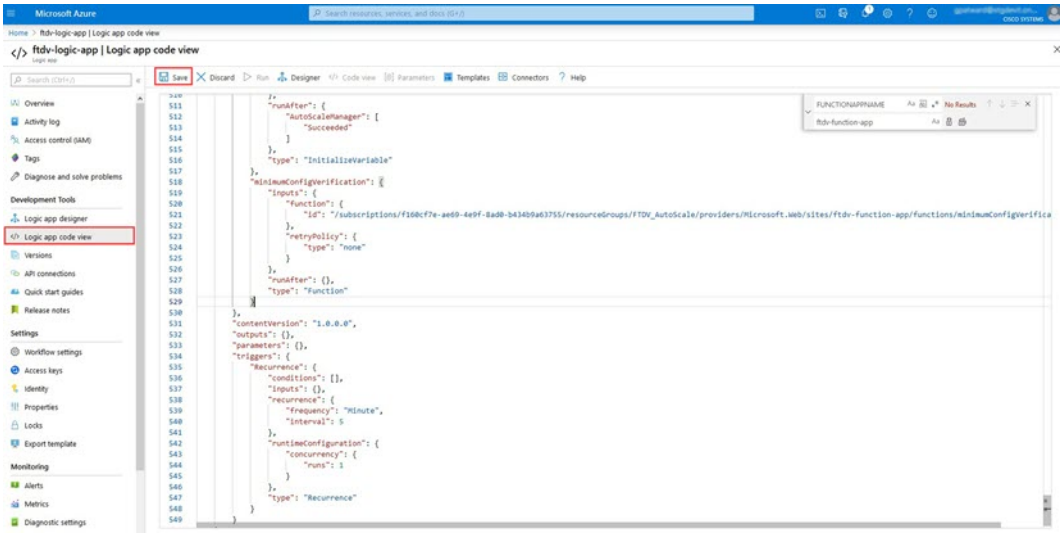
f) (Optional) Edit the cool down time, or leave the default value (10). This is the time to perform NO ACTION after the Scale-Out is complete. The following example shows these lines in the *LogicApp.txt* file:

```
    "actions": {
        "Branch_based_on_Scale-Out_or_Invalid_condition": {
            "actions": {
                "Cooldown_time": {
                    "inputs": {
                        "interval": {
                            "count": 10,
                            "unit": "Second"
                        }
```

Note
These steps can also be done from the Azure portal. Consult the Azure documentation for more information.

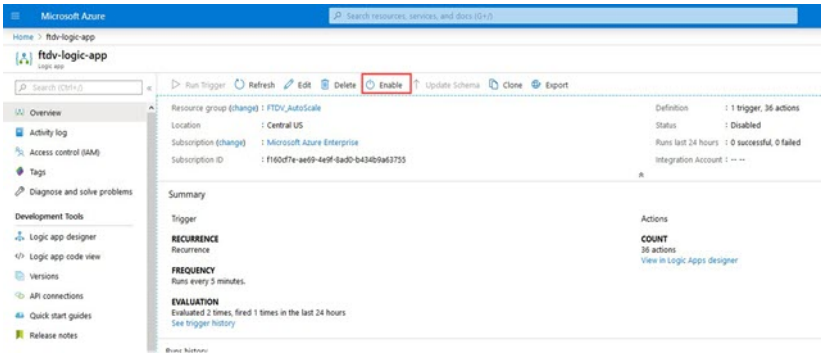
Step 2 Go to the **Logic App code view**, delete the default contents and paste the contents from the edited *LogicApp.txt* file, and click **Save**.

Figure 22: Logic App Code View



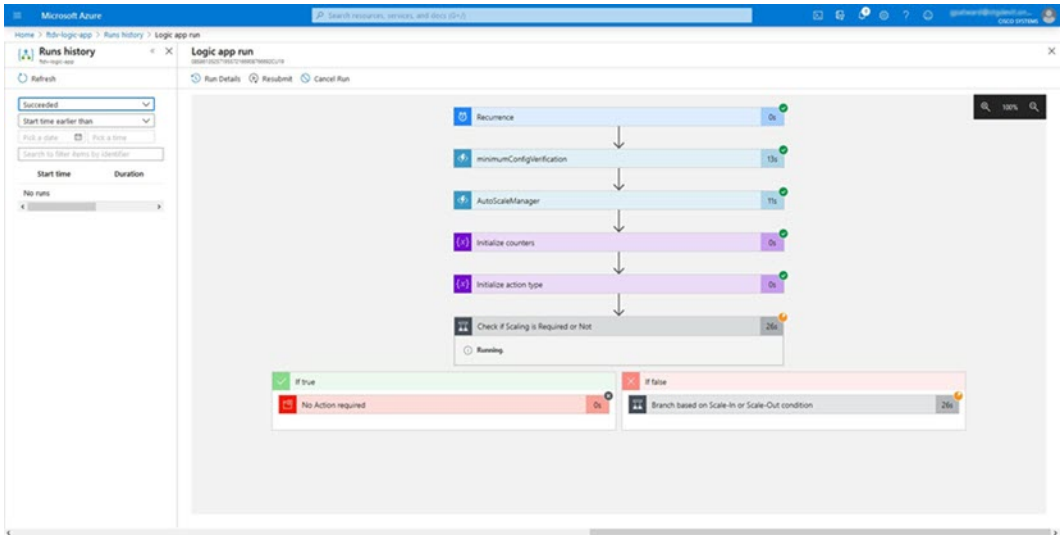
Step 3 When you save the Logic App, it is in a 'Disabled' state. Click **Enable** when you want to start the Auto Scale Manager.

Figure 23: Enable Logic App



Step 4 Once enabled, the tasks start running. Click the 'Running' status to see the activity.

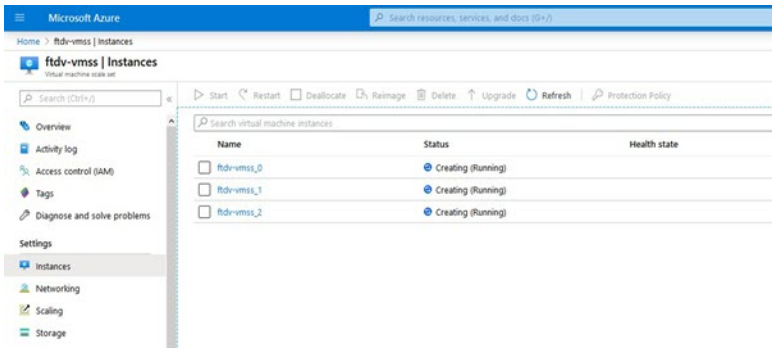
Figure 24: Logic App Running Status



Step 5 Once the Logic App starts, all the deployment-related steps are complete.

Step 6 Verify in the VMSS that threat defense virtual instances are being created.

Figure 25: Threat Defense Virtual Instances Running



In this example, three threat defense virtual instances are launched because 'minFtdCount' was set to '3' and 'initDeploymentMode' was set to 'BULK' in the ARM template deployment.

Upgrade the threat defense virtual

The threat defense virtual upgrade is supported only in the form of an image upgrade of virtual machine scale set (VMSS). Hence, you upgrade the threat defense virtual through the Azure REST API interface.

Note You can use any REST client to upgrade the threat defense virtual.

Before you begin

- Obtain the new threat defense virtual image version available in market place (example: 650.32.0).
- Obtain the SKU used to deploy original scale set (example: ftdv-azure-byol).
- Obtain the Resource Group and the virtual machine scale set name.

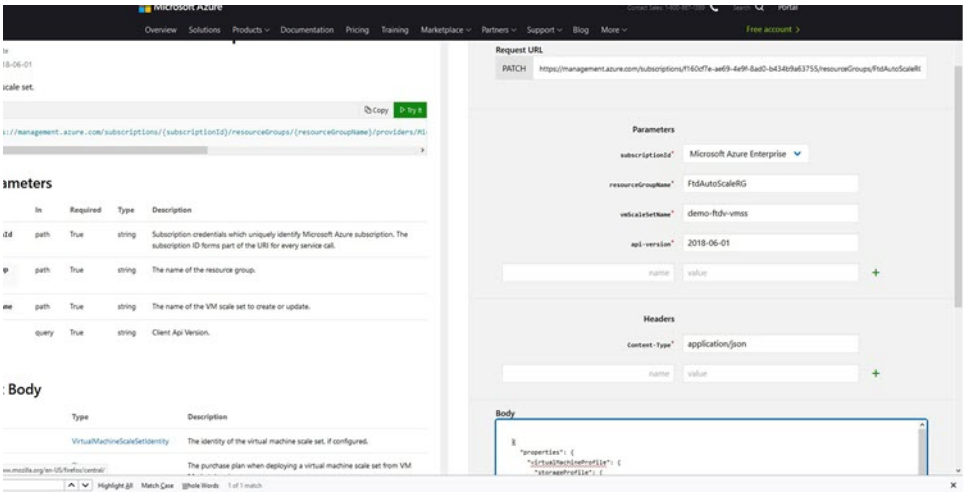
Procedure

Step 1 In a browser go to the following URL:

https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinescalesets/update#code-try-0

Step 2 Enter the details in the Parameters section.

Figure 26: Upgrade the threat defense virtual



Step 3 Enter the JSON input containing the new threat defense virtual image version, SKU, and trigger RUN in the **Body** section.

```
{
 "properties": {
        "virtualMachineProfile": {
              "storageProfile": {
                      "imageReference": {
                            "publisher": "cisco",
                            "offer": "cisco-ftdv",
                            "sku": "ftdv-azure-byol",
                             "version": "650.32.0"
                      }
                 },
            }
      }
}
```

Step 4 A successful response from Azure means that the VMSS has accepted the change.

The new image will be used in the new threat defense virtual instances which will get launched as part of Scale-Out operation.

- Existing threat defense virtual instances will continue to use the old software image while they exist in a scale set.
- You can override the above behavior and upgrade the existing threat defense virtual instances manually. To do this, click the **Upgrade** button in the VMSS. It will reboot and upgrade the selected threat defense virtual instances. You must reregister and reconfigure these upgraded threat defense virtual instances manually. **Note that this method is NOT recommended.**

Auto Scale Logic

Scaling Metrics

You use the ARM template to deploy the resources required by the threat defense virtualauto scale solution. During ARM template deployment, you have the following options for scaling metrics:

- CPU
- CPU, Memory (Version 6.7+).

Note CPU metrics are collected from Azure; memory metrics are collected from the management center.

Scale-Out Logic

- **POLICY-1**: Scale-Out will be triggered when the average load of **any** threat defense virtual goes beyond the Scale-Out threshold for the configured duration. When using the 'CPU,MEMORY' scaling metric, the Scale-Out threshold is the average CPU **or** memory utilization of **any** threat defense virtual in the scale set.
- **POLICY-2**: Scale-Out will be triggered when average load of **all** of the threat defense virtual devices go beyond Scale-Out threshold for the configured duration. When using the 'CPU,MEMORY' scaling metric, the Scale-Out threshold is the average CPU **or** Memory utilization of **all** threat defense virtual devices in the scale set.

Scale-In Logic

- If the CPU utilization of **all** of the threat defense virtual devices goes below the configured Scale-In threshold for the configured duration. When using the 'CPU,MEMORY' scaling metric, if the CPU **and** memory utilization of all threat defense virtual devices in the scale set goes below the configured Scale-In threshold for the configured duration, the threat defense virtual with the least loaded CPU will be selected for termination

Notes

- Scale-In/Scale-Out occurs in steps of 1 (i.e. only 1 threat defense virtual will be scaled in/out at a time).

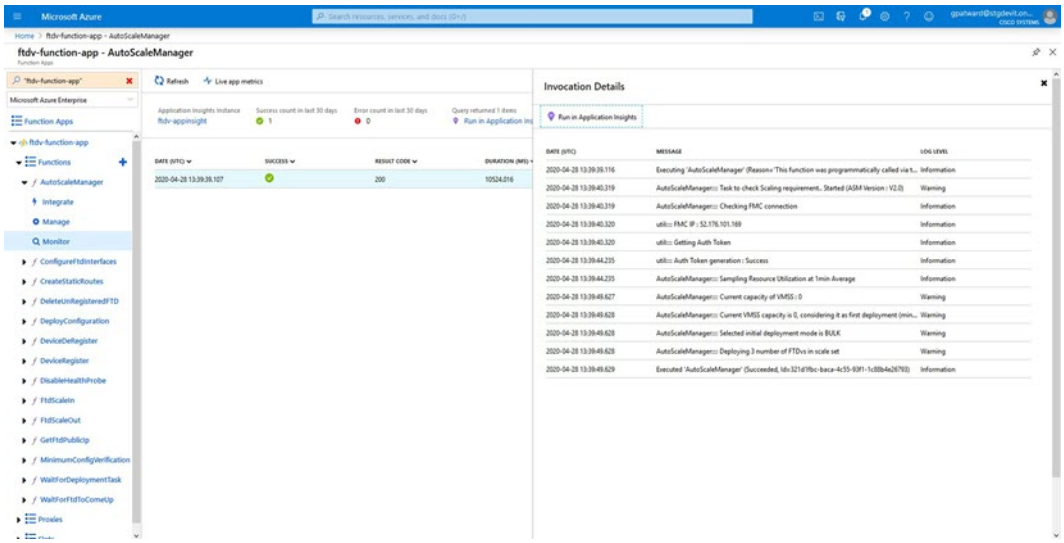
- The memory consumption metric received from the management center is not an average value calculated over time, but rather an instantaneous snapshot/sample value. Therefore, the memory metric alone cannot be considered in making scaling decisions. You do not have the option to use a memory-only metric during deployment.

Auto Scale Logging and Debugging

Each component of the serverless code has its own logging mechanism. In addition, logs are published to application insight.

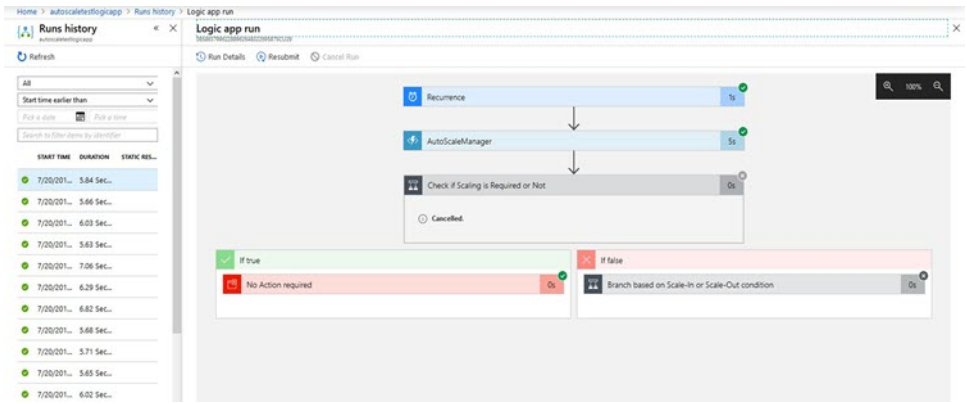
- Logs of individual Azure functions can be viewed.

Figure 27: Azure Function Logs



- Similar logs for each run of the Logic App and its individual components can be viewed.

Figure 28: Logic App Run Logs



- If needed, any running task in the Logic App can be stopped/terminated at any time. However, currently running threat defense virtual devices getting launched/terminated will be in an inconsistent state.
- The time taken for each run/individual task can be seen in the Logic App.

- The Function App can be upgraded at any time by uploading a new zip. Stop the Logic App and wait for all tasks to complete before upgrading the Function App.

Auto Scale Guidelines and Limitations

Be aware of the following guidelines and limitations when deploying the threat defense virtual auto scale for Azure:

- (Version 6.6 and earlier) Scaling decisions are based on CPU utilization.
- (Version 6.7+) Scaling decisions can use either CPU-only utilization, or CPU and memory utilization.
- Management Center management is required. Device Manager is not supported.
- The management center should have a public IP address.
- The threat defense virtual Management interface is configured to have public IP address.
- Only IPv4 is supported.
- Threat Defense Virtual auto scale for Azure only supports configurations such as Access policies, NAT policies, Platform Settings, etc. which are applied the Device Group and propagated to scaled-out threat defense virtual instances. You can only modify Device Group configurations using the management center. Device-specific configurations are not supported.
- The ARM template has limited input validation capabilities, hence it is your responsibility to provide the correct input validation.
- The Azure administrator can see sensitive data (such as admin login credentials and passwords) in plain text format inside Function App environment. You can use the *Azure Key Vault* service to secure sensitive data.
- Any changes in configuration won't be automatically reflected on already running instances. Changes will be reflected on upcoming devices only. Any such changes should be manually pushed to already existing devices.
- If you are facing issues while manually updating the configuration on existing instances, we recommend removing these instances from the Scaling Group and replacing them with new instances.

Troubleshooting

The following are common error scenarios and debugging tips for the threat defense virtual auto scale for Azure:

- Connection to the management center failed: Check the management center IP / Credentials; check if the management center is faulty / unreachable.
- Unable to SSH into the threat defense virtual: Check if a complex password is passed to the threat defense virtual via the template; check if Security Groups allow SSH connections.
- Load Balancer Health check failure: Check if the threat defense virtual responds to SSH on data interfaces; check Security Group settings.

- Traffic issues: Check Load Balancer rules, NAT rules / Static routes configured in threat defense virtual; check Azure virtual network / subnets / gateway details provided in the template and Security Group rules.
- The threat defense virtual failed to register with the management center: Check the management center capacity to accommodate new threat defense virtual devices; check Licensing; check the threat defense virtual version compatibility.
- Logic App failed to access VMSS: Check if the IAM role configuration in VMSS is correct.
- Logic App runs for very long time: Check SSH access on scaled-out threat defense virtual devices; check any device registration issues in management center; check the state of the threat defense virtual devices in Azure VMSS.
- Azure Function throwing error related to subscription ID : Verify that you have a default subscription selected in your account.
- Failure of Scale-In operation: Sometimes, Azure takes a considerably long time to delete an instance in such situations, Scale-in operation may time out and report an error; but eventually the instance, will get deleted.
- Before doing any configuration change, make sure to disable the logic application and wait for all the running tasks to complete.

The following are troubleshooting tips if you encounter any issues during threat defense virtual auto scale with Azure GWLB deployment:

- Check the ELB-GWLB association.
- Check the health probe status in the GWLB.
- Check VXLAN configuration by verifying the traffic flow at the physical and logical interfaces of the threat defense virtual.
- Check security group rules.

Build Azure Functions from Source Code

System Requirements

- Microsoft Windows desktop/laptop.
- Visual Studio (tested with Visual studio 2019 version 16.1.3)

Note Azure functions are written using C#.

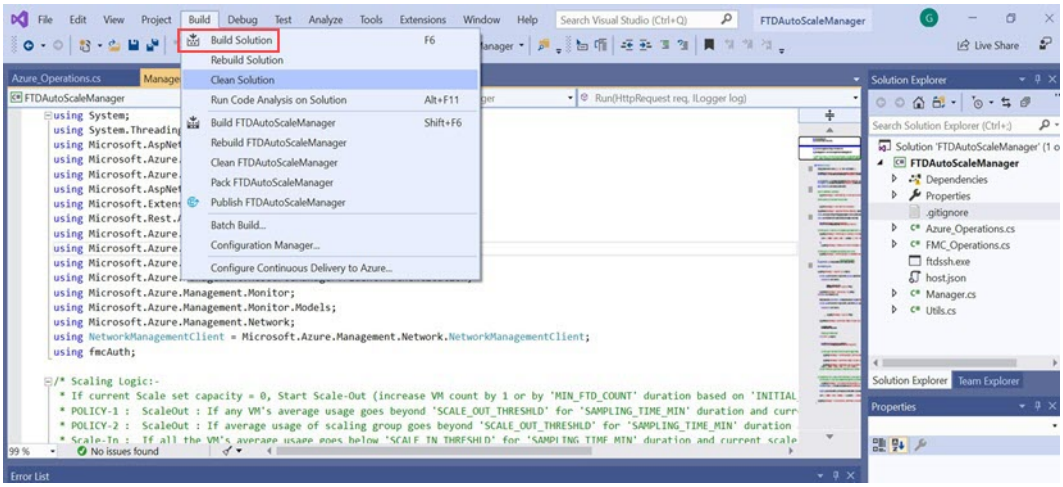
- The "Azure Development" workload needs to be installed in Visual Studio.

Build with Visual Studio

1. Download the 'code' folder to the local machine.

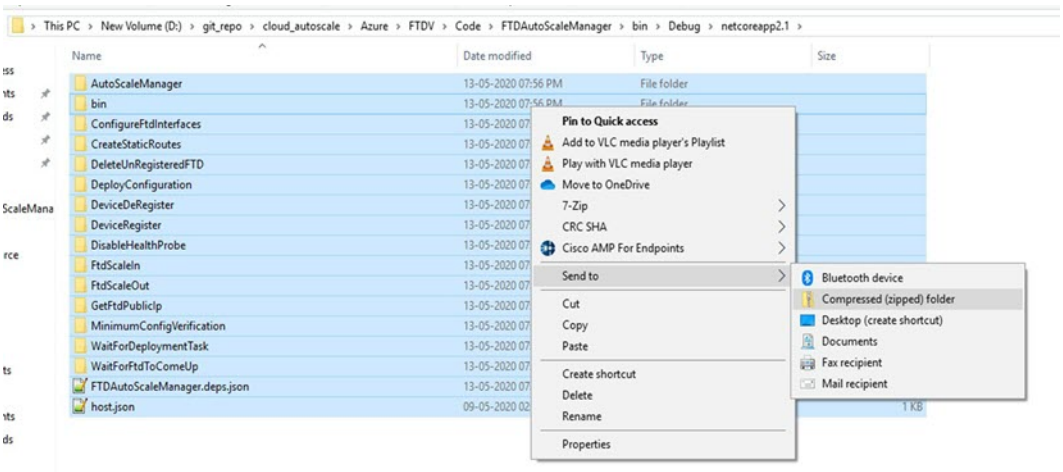
2. Navigate to the folder 'FTDAutoScaleManager'.
3. Open the project file 'FTDAutoScaleManager.csproj' in Visual Studio.
4. Use Visual Studio standard procedure to Clean and Build.

Figure 29: Visual Studio Build



5. Once the build is compiled successfully, navigate to the **\bin\Release\netcoreapp2.1** folder.
6. Select all the contents, click **Send to** > **Compressed (zipped) folder**, and save the ZIP file as *ASM_Function.zip*.

Figure 30: Build ASM_Function.zip



Deploy the Secure Firewall Threat Defense Virtual on Azure Virtual WAN

Introduction to Threat Defense Virtual in Azure Virtual WAN

Microsoft Azure Virtual WAN employs a 'hub-and-spoke' architecture to manage traffic across various virtual networks and branch locations. Within the Azure Virtual WAN, integrating Threat Defense Virtual with the Azure Virtual hub facilitates the efficient management and inspection of traffic originating from your organization's on-premises (spoke) networks (like headquarters, branches, and remote users) as it passes through the hub to access Vnets on your Azure network. This integration facilitates the management, inspection, filtering, and routing of network traffic through dedicated connectivity channels using Threat Defense Virtual functioning as firewall.

Note Threat Defense Virtual deployment model with only three interfaces is supported by Azure Virtual WAN.

Deploying Threat Defense Virtual on the Azure Virtual WAN hub offers several advantages, including:

- Eliminating the need to implement a firewall solution in each spoke connected to the hub.
- Leveraging Azure's inbuilt capabilities of Internal Load Balancer (ILB).
- Scaling of instances with predefined configuration during deployment.

For information about deploying the Threat Defense Virtual on the Virtual WAN hub, see Deploy Threat Defense Virtual on Azure Virtual WAN.

Traffic Routing Through Threat Defense Virtual on Azure Virtual WAN

Routing Traffic Methods in Azure Virtual WAN

Azure Virtual WAN offers Border Gateway Protocol (BGP), a dynamic routing protocol that helps determine the best route to send traffic between different Azure networks while constantly updating and sharing the routing table. The virtual WAN hub provides a set of BGP endpoints (for High Availability) and Autonomous System Number (ASN), which you must configure as BGP neighbors for Threat Defense Virtual in the management center.

You can also use the static routing method to manually configure routes in the Threat Defense Virtual.

For more information on routing in Azure, see About BGP and VPN Gateway in the Azure documentation.

Routing Intent

Routing Intent is a routing ability in the Azure Virtual WAN hub that simplifies the process of forwarding Internet-bound and Private traffic to the Threat Defense Virtual firewall deployed in the hub for inspection.

For more information, see Routing Intent in the Azure documentation.

System Requirements

Scaling Units

The scaling required to achieve maximum throughput depends on the instance size and number of Threat Defense Virtual instances (NVA) you select or configure during deployment in the Azure Virtual WAN hub.

For example: If two Threat Defense Virtual instances with **D3_V2** size can support 2.8 Gbps, then the NVA throughput is defined as **Scale-Unit-4: 2.8 Gbps**.

Table 3: Threat Defense Virtual Throughput Level Based on Instance Type

Scale Unit	Threat Defense Virtual instances	Instance Type	Throughput Support Level
4	2	Standard_D3_v2	3.2 Gbps
10	2	Standard_D4_v2	4.8 Gbps
20	2	Standard_D5_v2	12 Gbps
40	3	Standard_D5_v2	18 Gbps
60	4	Standard_D5_v2	24 Gbps
80	5	Standard_D5_v2	30 Gbps

Limitations

Interfaces

Threat Defense Virtual in an Azure Virtual WAN hub supports *Three* interfaces for deployment due to the restriction by Azure that an NVA can only support a maximum of three network interfaces.

Note Threat Defense Virtual version 7.4.1 and later that supports the three interface models is compatible for deployment on Azure Virtual WAN.

Three subnets for the Threat Defense Virtual network interfaces are as follows:

- **Management interfaces** – It is the **first interface** that connects the Threat Defense Virtual to the management center using a public IP address.
- **Outside interface (required)** - It is the **second interface** that connects the Threat Defense Virtual to an untrusted public IP address.
- **Inside interface (required)** - It is the **third interface** that connects the Threat Defense Virtual to the Virtual WAN hub and inside the host network on a trusted private IP address.

Threat Defense Virtual as Network Virtual Appliance (NVA)

The following are key features that are related to the network configuration of Threat Defense Virtual as NVA in Azure Virtual WAN.

- Azure internally creates the VNet and subnets during the deployment of Threat Defense Virtual on Azure Virtual WAN. As a result, you cannot modify or create them after the deployment is complete. However, you can view all the IP addresses attached to the instance after the deployment.
- You cannot choose the ports in network security groups for each interface, however, these ports are predefined during deployment. Only TCP ports 443, 8305, and 22 are allowed on the Management interface to connect to the internet.
- The Inside interface only allows communication within the Azure Virtual WAN hub and internal networks that are connected to it.

Access Restriction to Threat Defense Virtual on the Azure Virtual WAN Hub

You require authorization to access the Threat Defense Virtual instances that are deployed on the hub as a managed application into a managed resource group. The administrator can grant limited or restricted access to this managed resource group.

Azure managed applications offers a just-in-time (JIT) access feature that allows you to define access to managed applications. For information on the JIT, see Azure Managed Applications overview and just-in-time in the Azure documentation.

IP Support

- Only IPv4 is supported.

Unsupported Features

- Bootstrapping via Day 0 / Custom data is not supported.
- Threat Defense Virtual does not support streaming metrics to Azure.
- Virtual Machine upgrade by replacing the operating system disk is not supported.
- SSH key-based login to Threat Defense Virtual is not supported.
- PAYG is not supported.

Licensing

BYOL using a Cisco Smart License Account.

Network Topology

Threat Defense Virtual, as an NVA in the Azure Virtual WAN hub, inspects network traffic routing through the hub from different on-premises networks (spoke) such as Internet, Branch (Sites), or as VNETs.

These traffic routes through which the network traffic is traversing is categorized into the following topologies:

- East-West: Branch to Branch

- East-West: VNet to VNet
- North-South: Branch to Internet
- North-South: VNet to Internet

Note Traffic from **Internet to VNet or Branch** through Threat Defense Virtual is not supported in Secure Firewall version 7.4.1.

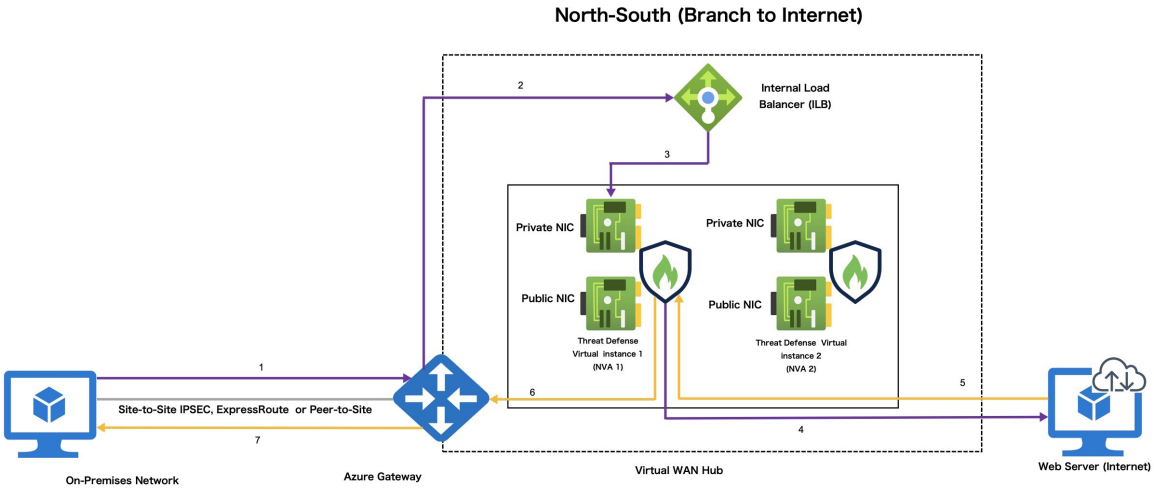
Note You can deploy multiple hubs across the Azure regions and connect to a Virtual WAN. Also, you can configure each hub to have its own Threat Defense Virtual for East-West and North-South traffic inspection.

North-South Traffic Inspection Topology by Threat Defense Virtual on a Single Virtual WAN Hub

This topology refers to Threat Defense Virtual inspecting the network traffic navigating between:

- Branches and VNETs, and vice versa are connected to the Virtual WAN hub.

Figure 31: Threat Defense Virtual North-South Traffic Inspection Topology in Azure Virtual WAN Hub



The following steps explain the traffic flow process in the North-South traffic inspection.

1. On-premises network sends traffic to Azure Gateway.
2. Gateway forwards to ILB.
3. ILB sends to Threat Defense Virtual (NVA)
4. NVA SNATS to instances PIP and sends to the Internet.
5. Web server replies to instance PIP Threat Defense Virtual (NVA) undoes SNAT and forwards to gateway.
6. Gateway forwards to on-premises network.

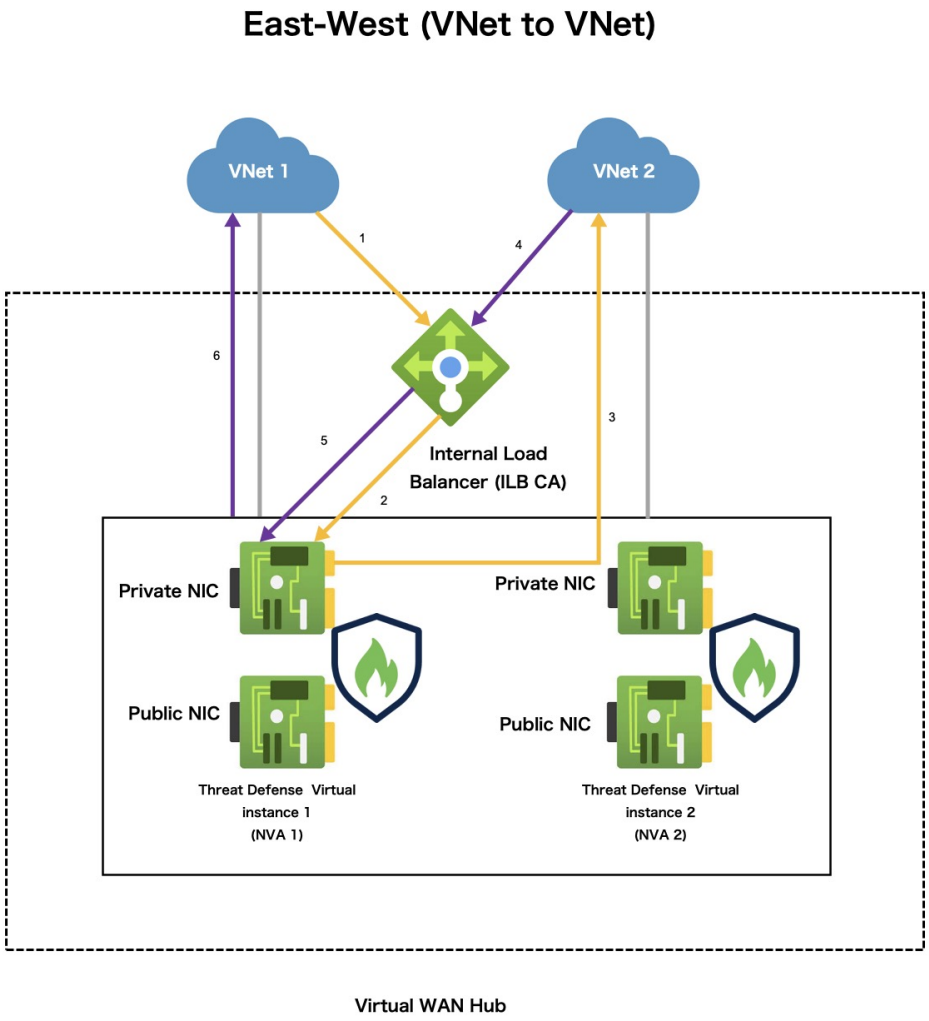
East-West Traffic Inspection Topology by Threat Defense Virtual on a Single Virtual WAN Hub

This topology refers to Threat Defense Virtual inspecting the network traffic navigating between:

- Branches and VNETs, and vice versa are connected to the Virtual WAN hub.
- Internet to Branch or VNETs connected to the Virtual WAN hub.

Figure 32: Threat Defense Virtual East-West Traffic Inspection Topology in Azure Virtual WAN Hub

This topology refers to Threat Defense Virtual inspecting the network traffic navigating between Site-to-Site (Branch and Branch) and VNET-to-VNET that are connected to the Virtual WAN hub.



The following steps explains the traffic flow process in the East-West traffic inspection.

1. VNet1 sends traffic to ILB.
2. ILB chooses one of the active instances.
3. Threat Defense Virtual (NVA) sends directly to the destination (VNet 2).

4. VNet sends traffic to ILB.
5. ILB forwards traffic to the appropriate Threat Defense Virtual (NVA) state fully.
6. Threat Defense Virtual (NVA) sends traffic back to VNet 1.

Deploy Threat Defense Virtual on Azure Virtual WAN

You can use the Cisco Secure Firewall Threat Defense Virtual for Azure Virtual WAN offering that is available on Azure Marketplace to deploy Threat Defense Virtual on the Azure Virtual WAN hub.

Prerequisites

- A Microsoft Azure account. You can create one at https://azure.microsoft.com/en-us/.
- Create a hub on your Virtual WAN. For information on creating a virtual hub in Azure, see Create a hub in the Azure documentation.
- Ensure that the Virtual WAN hub address space is less than or equal to /23.

Note Microsoft Azure allows Virtual WAN hubs with /24 address spaces. However, Microsoft does not recommend the deployment of such hubs due to future enhancements. We do not support deploying Threat Defense Virtual in a Virtual WAN hub with a /24 address space.

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

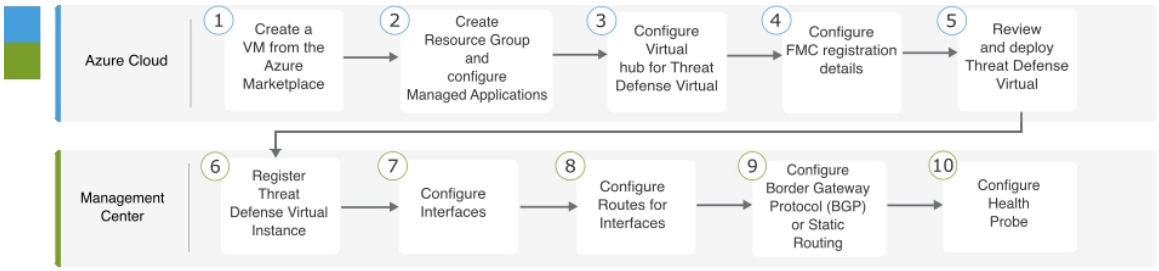
Note Post deployment of Threat Defense Virtual instances, you can view all the public and private IPs attached to the instance.

Communication Paths

- Management interface—Used to connect the Threat Defense Virtual to the Management Center.
- Inside interface (required)—Used to connect the Threat Defense Virtual to inside hosts.
- Outside interface (required)—Used to connect the Threat Defense Virtual to the public network.

End-to-End Procedure

The following flowchart illustrates the workflow for deploying the Threat Defense Virtual on Azure Virtual WAN using the Solution template.



	Workspace	Steps
1	Azure Cloud	Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template: Search for "Cisco Secure Firewall Threat Defense Virtual for Azure VWAN" in the Azure Marketplace.
2	Azure Cloud	Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template: Create Resource Group and configure Managed Applications.
3	Azure Cloud	Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template: Configure the Virtual hub and the NVA details.
4	Azure Cloud	Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template: Configure FMC registration details.
5	Azure Cloud	Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template: Review and deploy Threat Defense Virtual.
6	Management Center or Device Manager	Register Threat Defense Virtual Instances in the Management Center: Register the Threat Defense Virtual instance.
7	Management Center or Device Manager	Configure Interfaces: Configure Outside and Inside interfaces.
8	Management Center or Device Manager	Configure Route for Interfaces: Compute gateway IP address, and configure the routes for Outside and Inside interfaces.
9	Management Center or Device Manager	Configure Traffic Routing: Configure Border Gateway Protocol (BGP) or static routing
10	Management Center or Device Manager	Configure Health Probe: Configure health probe to enable ILB for performing periodic health check of Threat Defense Virtual instances.

Deploy Threat Defense Virtual on Azure Virtual WAN Using Solution Template

The following instructions show how to deploy the Threat Defense Virtual on Azure Virtual WAN using the solution template that is available in the Azure Marketplace. This is a top-level list of steps to set up the Threat Defense Virtual in the Microsoft Azure Virtual WAN environment.

For more information about the Azure setup, see Getting Started with Azure.

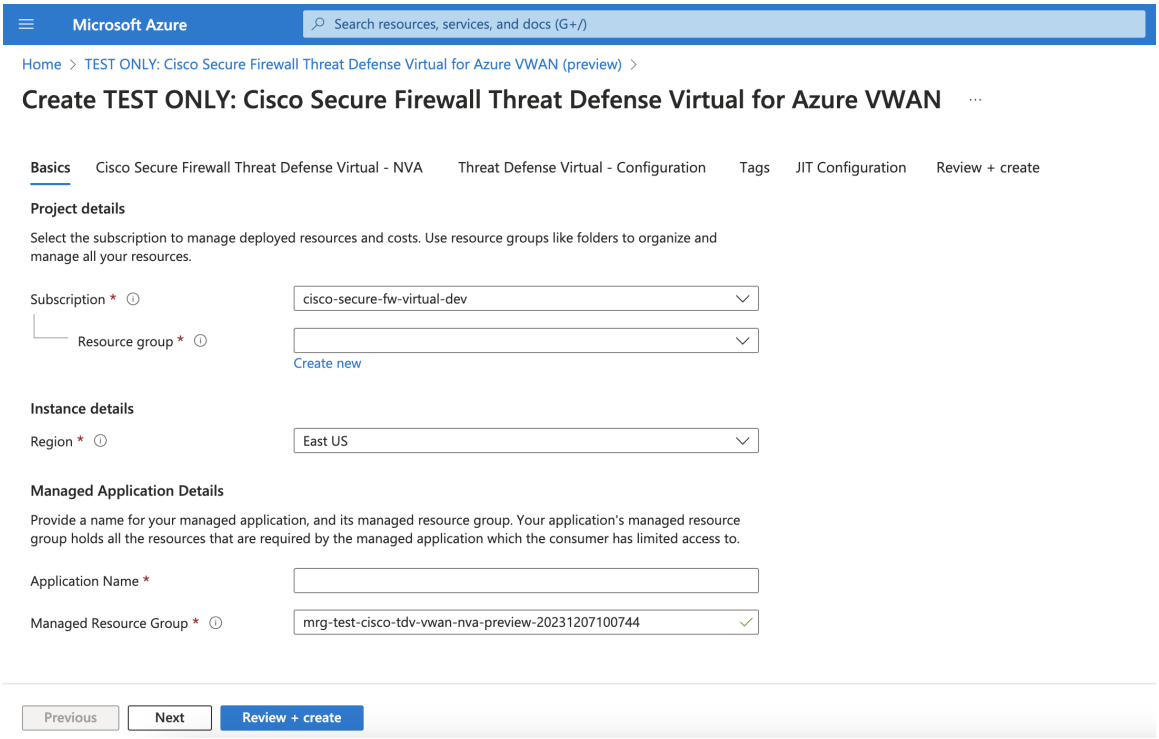
Procedure

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

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

Step 2 Choose **Azure Marketplace** > **Virtual Machines**.

Step 3 Search the Marketplace for **Cisco Secure Firewall Threat Defense Virtual for Azure VWAN**, choose the offering, and click **Create**to display the **Basics** page.



Step 4 Configure the **Basics** settings.

a) Choose your subscription.

b) Create a new **Resource Group**.

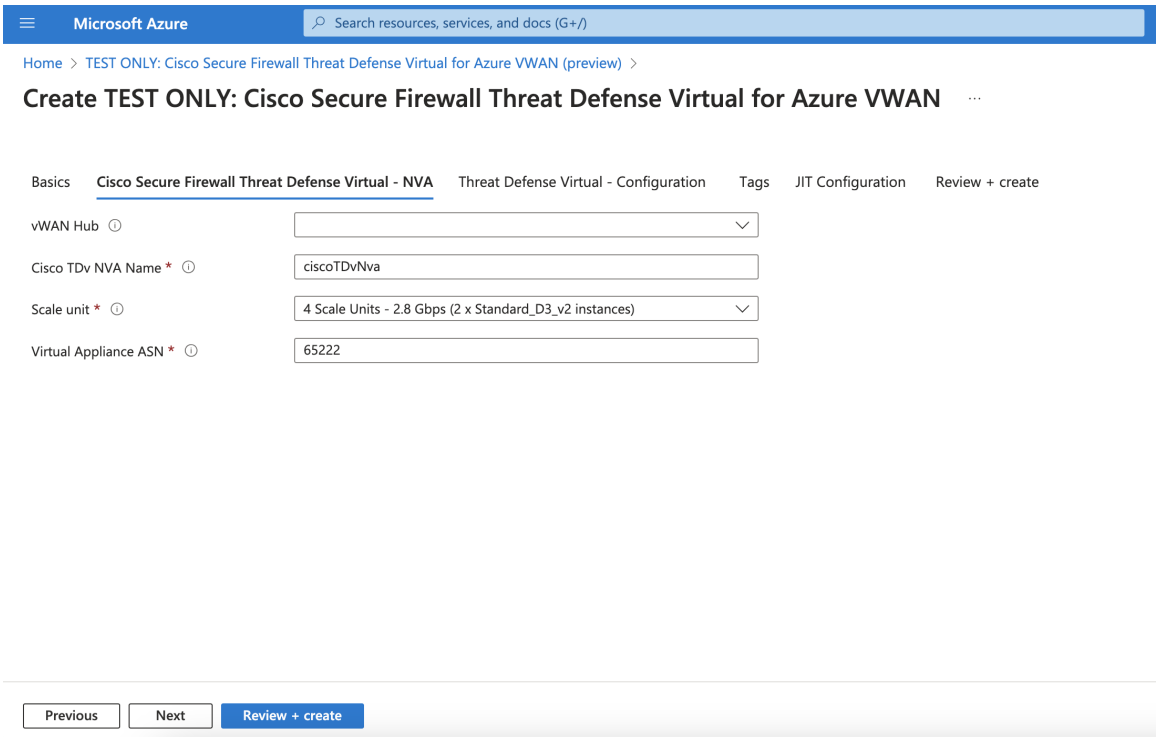
c) Select the geographical location or region of the Virtual WAN hub. It should be the same for all the resources that are used in this deployment (for example VIRTUAL WAN hub, Threat Defense Virtual, Network, storage accounts).

Step 5 Configure **Managed Application Details** settings.

a) Enter a name for the Managed Application of the managed resource group where you are deploying the Threat Defense Virtual instance as NVA.

b) Select the managed resource group where you deploy the Threat Defense Virtual instance.

Step 6 Click **Next** to display the **Cisco Secure Firewall Threat Defense Virtual - NVA** page.



Step 7 Configure the Virtual hub and the NVA details:

a) Select the Virtual WAN hub from the **vWAN Hub** drop-down list to deploy a Threat Defense Virtual instance.

b) Enter an appropriate name for the Threat Defense Virtual instance you are deploying.

c) Select the scale units that define the number of Threat Defense Virtual instances you want to deploy.

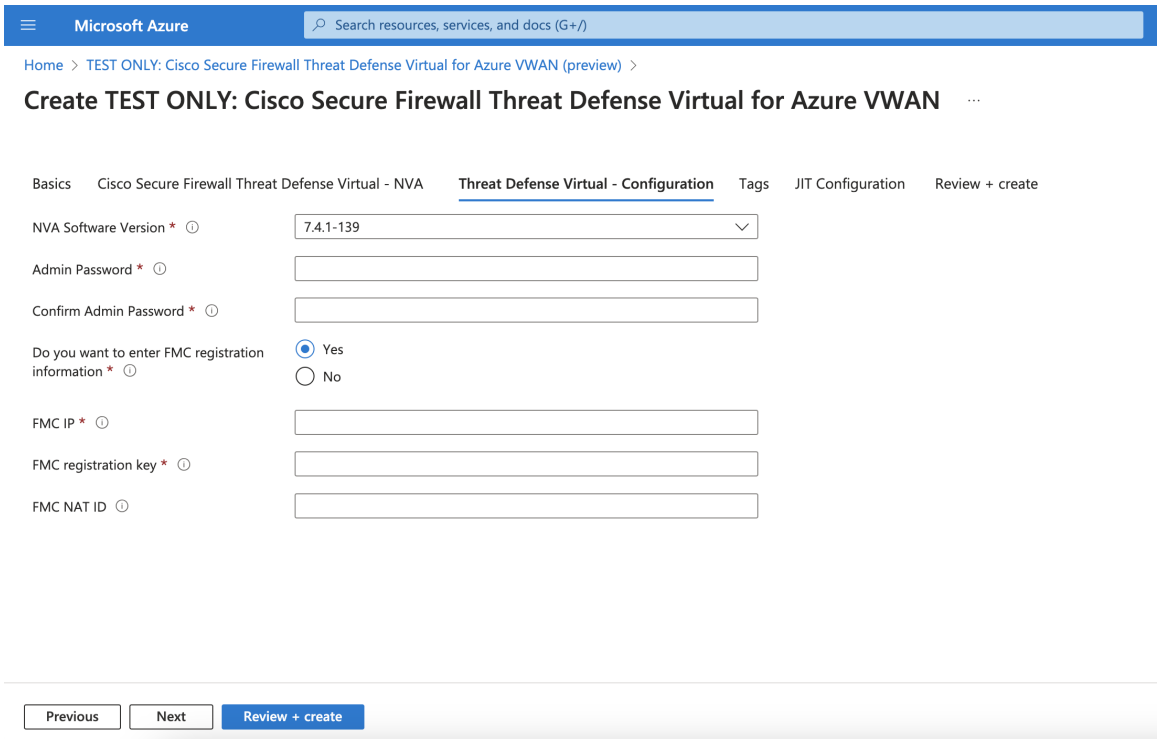
You can select the required scale unit to achieve the needed NVA throughput level. For example, selecting **4 Scale Units – 2.8 Gbps** (**2 x Standard_D3_v2_instances**) implies "**Number scale unit** – **Throughput level** (**2 Threat Defense Virtual with instance type**).

Note
Scale unit defines the number of Threat Defense Virtual instances and its associated instance type that you are deploying in the hub.

d) Enter the **Virtual Appliance ASN**.

Note
The ASN value that you enter must be within the range 64512 – 65534.

Step 8 Click **Next** to display the **Threat Defense Virtual - Configuration** page.



Step 9 Select the appropriate **NVA Software version** compatible version from the drop-down list.

Note
This field provides a list of NVA software versions compatible with the corresponding Threat Defense Virtual version you are deploying. Ensure to select the appropriate version from the list.

Step 10 Create and confirm the admin password that is required to access the managed resource group containing Threat Defense Virtual instances.

Step 11 Click **Yes** to enter the **FMC registration information**.

a) Enter the **FMC IP** address.

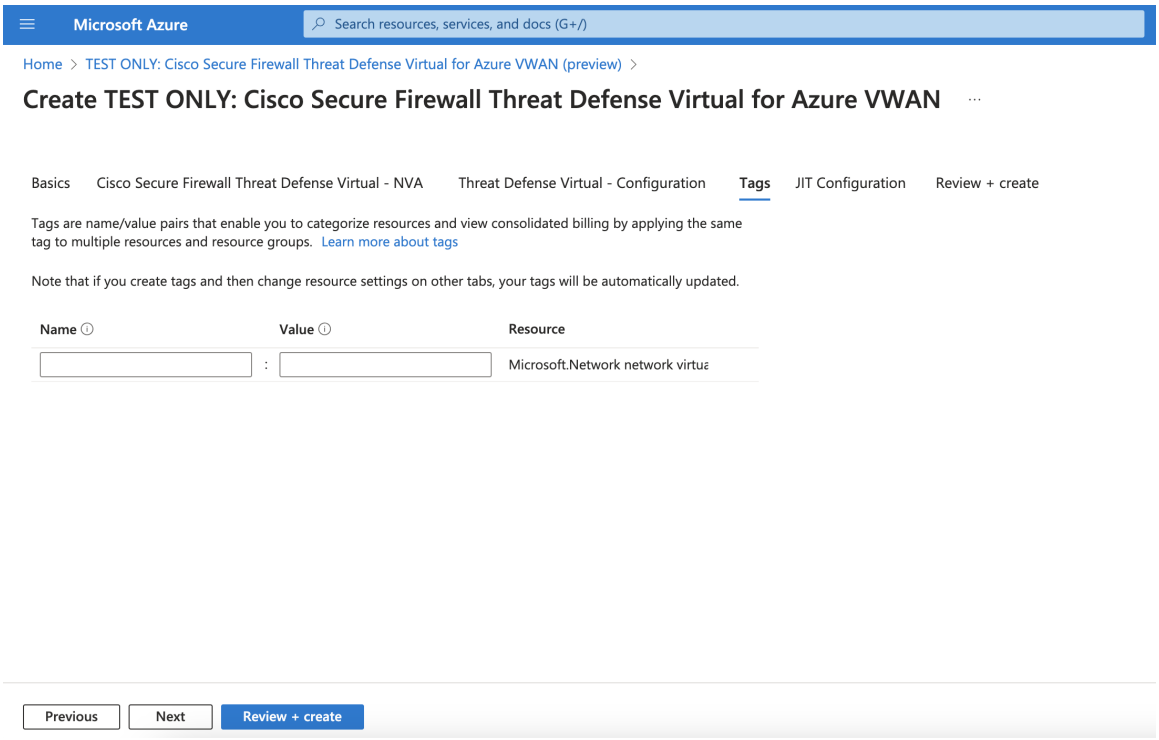
b) Enter the **FMC Registration Key** for registering the Threat Defense Virtual instances.

Note
- The FMC Registration key must be an alphanumeric string of 1 – 37 characters in length. You will enter this key on the Management Center when adding Threat Defense Virtual.

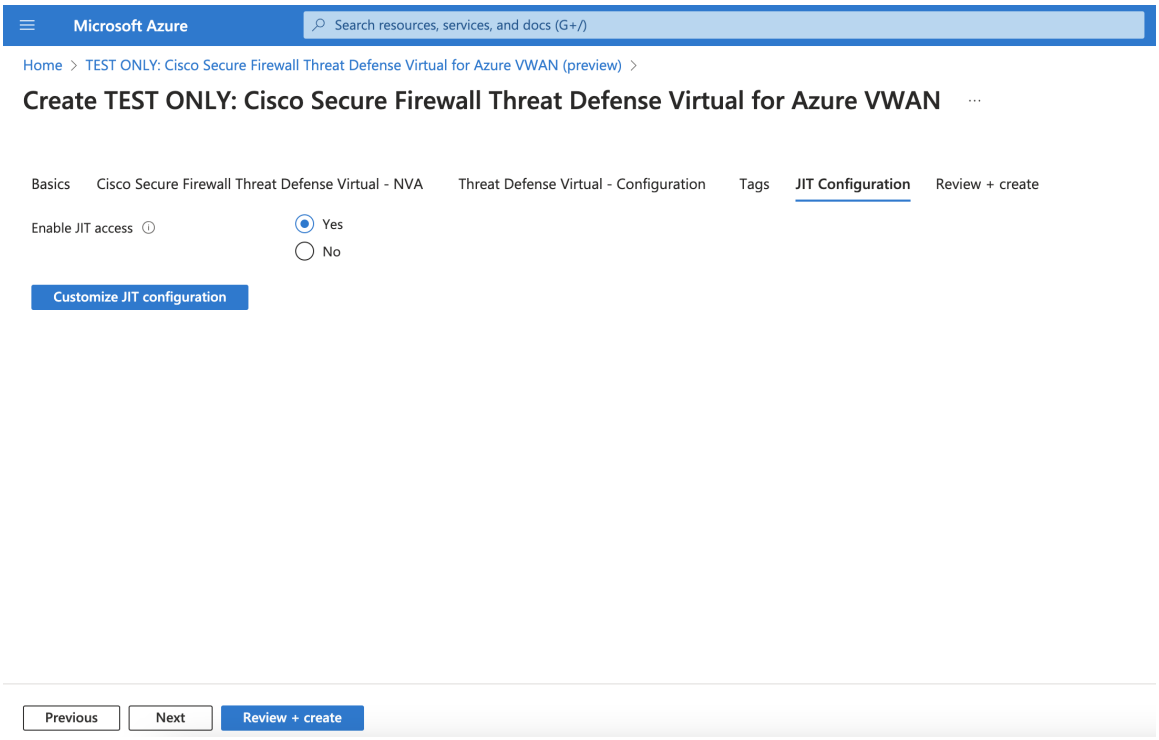
c) [Optional] Enter the management center NAT ID that is used during instance registration.

Note
- The NAT ID must be an alphanumeric string between 1 – 37 characters in length and is used only during the registration process between the Management Center and the device when one side does not specify an IP address. The NAT ID is essentially a one-time password, so it must be unique and not used by any other devices awaiting registration. To ensure successful registration, be sure to specify the same NAT ID on the FMC when adding the Threat Defense Virtual.

Step 12 Click **Next** to configure the **Tags**.

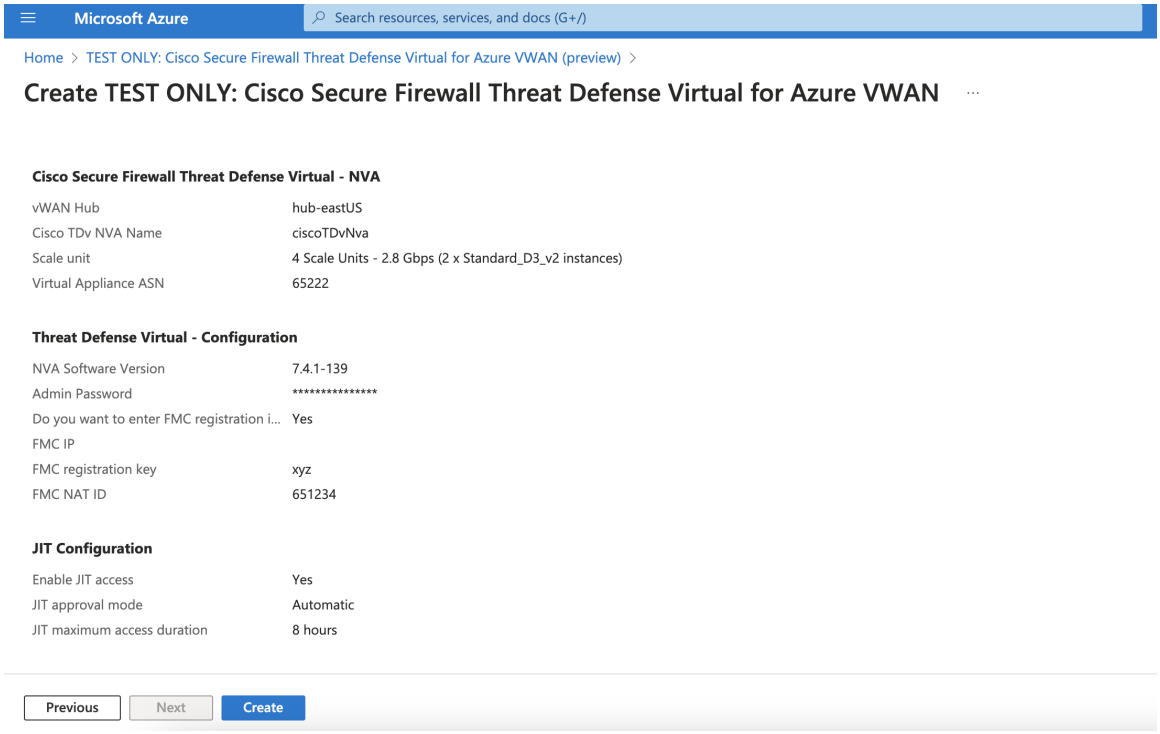


Step 13 Click **Next** to display the **JIT configuration** page.



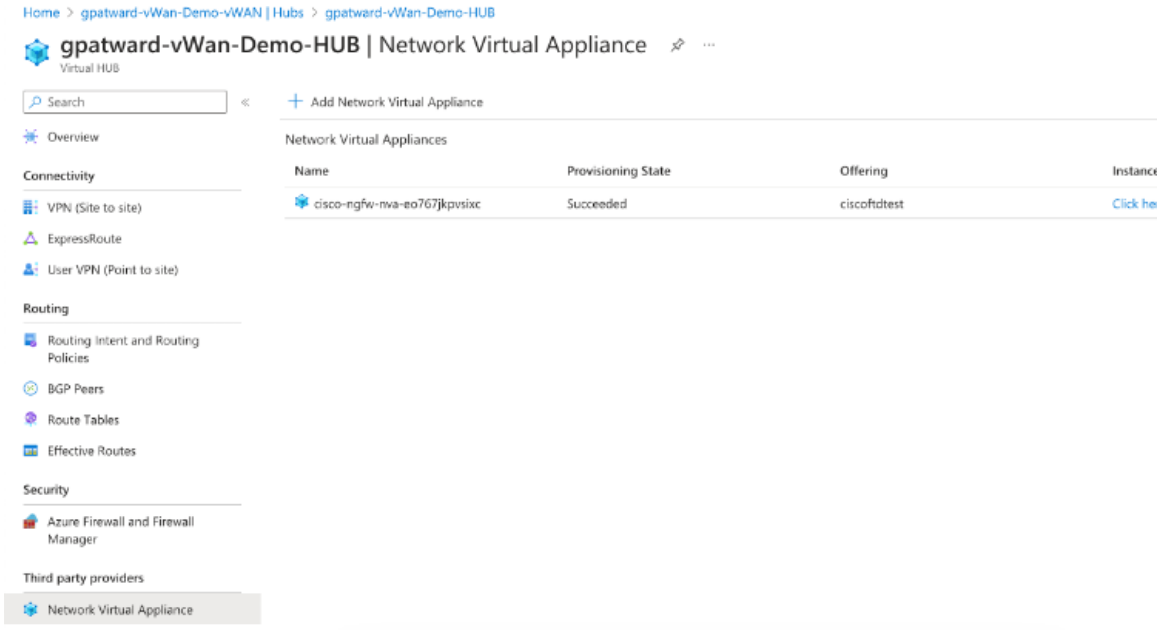
By default, the **Enable JIT access** option is set to **Yes**, which enables JIT for provisioning access to manage and troubleshoot the Threat Defense Virtual instances.

Step 14 Click **Next** to display the **Review+Create** page.



Step 15 Before deploying, you must review the subscription, NVA, Threat Defense Virtual and JIT configuration details, accept the Terms and conditions and then click **Create** to deploy the Threat Defense Virtual (NVA) on the Virtual WAN hub.

Step 16 Go to **Home** > **Security** > **Third-party providers**, and click **Network Virtual Appliance** to view the NVA created on the hub.



Step 17 Click the **NVA** to view all the Threat Defense Virtual instances deployed.

You can access the Threat Defense Virtual using the management public IP address of the instance and login using the SSH.

Note
The public IP addresses of each Threat Defense Virtual instance that you deploy on the hub is used for registering the instances in the management center.

What to do next

Register and configure the Threat Defense Virtual instances that you deployed on the hub in the management center.

Configure Threat Defense Virtual in Management Center

You configure each Threat Defense Virtual instance deployed on the hub through the management center.

Create all the objects needed for the Threat Defense Virtual configuration and management, including a device group, so you can easily deploy policies and install updates on multiple devices. All the configurations applied on the device group will be pushed to the Threat Defense Virtual instances.

This section provides a brief overview of the basic steps to configure the Threat Defense Virtual instances in the management center.

For more information, see Cisco Secure Firewall Management Center Device Configuration Guide.

Register Threat Defense Virtual Instances in the Management Center

You must register all the Threat Defense Virtual instances that are deployed in the virtual WAN hub under a common Device group in the management center. It helps you to quickly deploy policies and configurations to those instances.

Before you begin

- Require the management public IP address of each Threat Defense Virtual instance deployed in the Azure Virtual WAN hub. It is used to set up and register instances in the management center.
- Create a Device Group in the management center. See Add a Device Group.
- Create an Access Control Policy. See Creating a Basic Access Control Policy.
- FMC Registration Key created during Threat Defense Virtual deployment in the hub.

Procedure

Step 1 Log in to the Management Center.

Step 2 Choose **Devices** > **Device Management**.

Step 3 Click **Add** > **Device**

Step 4 Enter the public IP address of the Threat Defense Virtual instance deployed in the hub.

Step 5 Provide the display name for the Threat Defense Virtual instance.

Step 6 Enter the **Registration Key** of the management center that you have created during the Threat Defense Virtual deployment in the hub.

Step 7 From the **Group** drop-down list, choose the device group to which you want to add the Threat Defense Virtual instance.

Step 8 From the **Access Control Policy** drop-down list, select the policy that you want to apply to the Threat Defense Virtual instance.

Step 9 Enter other details as required.

Step 10 Click **Register**.

Step 11 Repeat Step 1 through Step 10 to register other Threat Defense Virtual instances.

What to do next

Configure interfaces of Threat Defense Virtual instances.

Configure Interfaces

After registering the Threat Defense Virtual instance, you must configure its interfaces in the management center.

The Azure Virtual WAN supports only **three** interfaces, which is configured as follows:

- Management interface with the public IP as the first interface.
- Outside interface with the public IP as the second interface.
- Inside interface with the private IP as the third interface (which has only private IP).

Procedure

Step 1 Log in to the Management Center.

Step 2 Go to the **Devices** page.

Step 3 Click the **Edit** icon corresponding to the Threat Defense Virtual you have registered.

Step 4 Click the **Edit** icon corresponding to an interface. For example, **GigbitEthernet0/0**.

Step 5 Enter the name of the first interface as **`outside`**.

Step 6 Check the **Enabled** check box to enable the interface.

Step 7 From the **Security Zone** drop-down list, select **outside**.

Step 8 Click the **IPv4** menu to assign the type of IP to the interface.

Step 9 From the **IP Type** drop-down list, select **Use DHCP** to configure your interface to obtain an IP address from DHCP.

Step 10 Check the **Obtain default route using DHCP** check box.

Step 11 Enter the **Default route** metric as **`1`**.

Step 12 Click **OK** to save the configuration.

Step 13 Repeat Step 1 through Step 10 to configure the Inside interface.

What to do next

Configure routes for interfaces.

Configure Route for Interfaces

Configure the static routes for Outside and Inside interfaces by creating network objects and assigning the gateway IP address.

- The Outside interface route configuration uses the gateway IP address as the default route for all the packets.
- The Inside interface route configuration uses the gateway IP address as the default route for the health probe packets and the packets that are destined for the hub network range.

The gateway IP address is computed using each interface's IP address and subnet mask address.

Compute Gateway IP Address for Outside and Inside Interface

This section explains the process of computing the gateway IP address for the Outside and Inside interfaces with an example.

Procedure

Step 1 Log in to the Management Center.

Step 2 Go to the **Devices** > **Device Management**.

Step 3 Access the Threat Defense Virtual instance you have deployed on the hub.

Step 4 In the **>_Command** field, enter **`show interface GigbitEthernet 0/0`** to get the Outside interface configuration or **`show interface GigbitEthernet 0/1`** to get the Inside interface configuration details.

Step 5 Repeat Step 1 through Step 4 to get the IP address and subnet mask addresses for the Inside interface or Outside interface.

Step 6 Note the IP address and subnet mask addresses from the command result.

Step 7 Compute the gateway IP addresses for Inside and Outside by following the example:

- To compute gateway IP address for Outside interface:

  For Example: For GigabitEthernet0/0 (Outside interface)

  IP address - **15.0.112.136**

  Subnet mask - **255.255.255.128**

  Hence, compute the gateway IP address as (that is the first IP address in this subnet) **15.0.112.129**.

- To compute gateway IP address for Inside interface:

  For Example: For GigabitEthernet0/1 (Inside interface)

  IP address - **15.0.112.10**

  Subnet mask - **255.255.255.128**

Hence, compute the gateway IP as (that is the first IP address in this subnet) **15.0.112.1**.

What to do next

Configure default route for Inside and Outside interfaces.

Configure Default Route for Outside Interface

Procedure

Step 1 Log in to the Management Center.
Step 2 Go to the **Devices** > **Device Management**.
Step 3 Click the Threat Defense Virtual instance.
Step 4 Click **Routing** > **Static Route**.
Step 5 Click **Add Route**.
Step 6 From the **Interface** drop-down list, select **Outside**.
Step 7 Select **any-ipv4** for the Outside interface under **Available Network** and click **Add**.
Step 8 Enter the gateway IP address:
a) Click the + icon to add a network object.
b) Enter the name and description of the network object.
c) Click the **Host** network.
d) Enter the gateway IP address of the Outside interface that you have computed.
e) Click **Save**.

Configure Default Route for Inside Interface

Before you begin

You must have the CIDR IP address of the Threat Defense Virtual deployed on the hub. You require this to configure the Inside interface.

Procedure

Step 1 Log in to the Management Center.
Step 2 Go to the **Devices** > **Device Management**.
Step 3 Click the Threat Defense Virtual instance.
Step 4 Click **Routing** > **Static Route**.
Step 5 Click **Add Route**.
Step 6 From the **Interface** drop-down list, select **Inside**.

Step 7 Add the network object to configure the Inside interface with the CIDR IP address of the hub.

a) Click the + icon to add a network object.
b) Enter the name and description of the network object.
c) Click the **Host** network.
d) Enter the CIDR IP address (Private address space) of the hub.
e) Click **Save**.

Step 8 Add the network object to configure the Inside interface with the load balancer health probe IP address.

a) Click the + icon to add a network object.
b) Enter the name and description of the network object.
c) Click the **Host** network.
d) Enter the IP address of the load balancer health probe. For example:`168.63.129.16`.

This IP address is a standard or fixed address.

Step 9 Enter the gateway IP address:

a) Click the + icon to add a network object.
b) Enter the name and description of the object.
c) Click the **Host** network.
d) Enter the gateway IP address of the Inside interface that you have computed.
e) Click **Save**.

Configure Traffic Routing

You can configure either a static routing or Border Gateway Protocol (BGP) for data exchange between the Threat Defense Virtual instances and the hub. It is essentially two different routing methods that you can configure for the network traffic in a Virtual WAN hub.

BGP is a dynamic routing protocol that factors the route based on the real-time traffic exchange between the hub and your threat defense virtual appliance. Whereas the static routing uses a preconfigured routing protocol to exchange traffic.

For more information about Azure Virtual WAN, refer to the Microsoft Azure Virtual WAN documentation.

Configure Static Routing

Procedure

Step 1 Log in to the Management Center.

Step 2 Go to the **Devices** > **Device Management**.

Step 3 Click the Threat Defense Virtual instance.

Step 4 Click **Routing** > **Static Route**.

Step 5 Click **Add Route**.

Step 6 From the **Interface** drop-down list, select **Outside**.

If you are configuring the Inside interface, select **Inside**.

Step 7 Add the network object IP address:

a) Click the + icon to add a network object.
b) Enter the name and description of the object.
c) Click the **Host** network.
d) Enter the IP address.
e) Click **Save**.

Enable BGP Routing

Procedure

Step 1 Log in to the Management Center.
Step 2 Choose **Devices** > **Device Management**.
Step 3 Click the Threat Defense Virtual instance.
Step 4 Click the **Routing** menu.
Step 5 Click **BGP** under **General Settings**.
Step 6 Check the **Enable BGP** check box.
Step 7 Enter the AS number of your virtual hub.
Step 8 Click **Save**.

What to do next

Configure BGP neighbors.

Configure BGP Neighbors

Procedure

Step 1 Log in to the Management Center.
Step 2 Choose **BGP** > **IPv4** > **Neighbor**.
Step 3 Check the **Enable IPv4** check box.
Step 4 Enter the Autonomous System (AS) number of your virtual hub.
Step 5 Click **Add** in the Neighbor.
Step 6 Enter the first IP address of the BGP endpoint that you have noted.
Step 7 Check the **Enabled address** check box.
Step 8 Enter the AS number in the **Remote AS** field.
Step 9 Check the **Disable Connection Verification** check box on the **Advanced** menu.
Step 10 Click **Save**.

Step 11 Repeat Step 1 through Step 8 to add the second IP address of the BGP endpoint.

What to do next

Verify BGP route configuration.

Verify BGP Route Configuration

Before you begin

After configuring the BGP endpoints, you must verify whether a connection through the BGP endpoints is established between Threat Defense Virtual and the virtual WAN hub.

Procedure

Step 1 Log in to the Management Center.
Step 2 Choose **Devices** > **Device Management**.
Step 3 Click the Threat Defense Virtual instance.
Step 4 Click **CLI** in the **Device** > **General** widget.
Step 5 In the **>_Command** field, enter **show route** to view and verify the connection status.

Note
Code **B** indicates the BGP endpoint connection status with the Threat Defense Virtual.

Configure Health Probe

To ensure the Threat Defense Virtual status is stable, you must configure the Inside interface (Trusted) that connects to the Internal Load Balancer (ILB). The ILB performs periodic health check probes through the TCP port 443 to verify the response from Threat Defense Virtual.

Procedure

Step 1 Log in to the Management Center.
Step 2 Choose **Devices** > **Platform Settings** > **New Policy** > **Threat Defense Settings**.
Step 3 Add a **New policy** for the Threat Defense Virtual to connect to the load balancer.
Step 4 Edit the new policy that you have added.
Step 5 Check the **Enable HTTP Server** check box, and enter `443` in the **Port** field.
Step 6 Click **+ Add** to configure the HTTP address.
Step 7 Select the health probe IP address name.
Step 8 Select the required IP address from the **Available Zone/Interface** and click **Add** to add it to **Selected Zones/Interfaces**.
Step 9 Click **OK**.

Step 10 Choose **Devices** > **Device Management**.

Step 11 Click the edit icon in the **Applied Policies** widget.

Step 12 Select this policy from the **Platform Settings** drop-down list.

Step 13 Update and apply the security policies as required.

For more information about configuring HTTP Access, see Configuring HTTP.

Troubleshooting

The following are common error scenarios and debugging tips for the Threat Defense Virtual in Virtual WAN:

- Traffic is not routed to Threat Defense Virtual.
  - Verify the Threat Defense Virtual response to health probe checks in the management center.
  - Verify whether the derived gateway IP addresses of the Inside and Outside interfaces are correct.
  - Check the static route.
- Non-RFC RFC 1918 not reaching Threat Defense Virtual: Ensure Non-RFC 1918 ranges that are explicitly specified as Private addresses in the Routing Intent.
- Threat Defense deployment error: If you encounter the Error: **Hub Prefix Length should be less or equal to 23** during Threat Defense Virtual deployment, then ensure that the CIDR of the HUB address space is less than or equal to **/23**.

Deploy the IPv6 Supported Secure Firewall Threat Defense Virtual on Azure

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

About IPv6 Supported Deployment on Azure

Threat Defense Virtual offerings support both IPV4 and IPv6 from 7.3 and later. In Azure, you can deploy 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 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 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 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 threat defense virtual . To use this template, see Deploy from Azure Using Custom IPv6 Template with Marketplace Image Reference, on page 86.

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 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 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 threat defense virtual . See, Deploy from Azure Using a VHD and Custom IPv6 Template, on page 91.

The process involved in deploying 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 threat defense virtual is as follows:

Table 4:

Step	Process
1	Create a Linux VM in Azure where you are planning to deploy the IPv6-supported threat defense virtual
2	Enable Programmatic deployment option on Azure portal or Azure CLI **only** when you are deploying 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 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 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 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 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 threat defense virtual .

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

Step 4 Select one of the threat defense virtual version from the list of available marketplace image versions that are displayed.

For IPv6 support deployment of threat defense virtual , you must select the 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 threat defense virtual custom deployment:

Parameter Name	Examples of allowed Values/Type	Description
vmName	csf-tdv	Name the threat defense virtual VM in Azure.
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 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

Parameter Name	Examples of allowed Values/Type	Description
		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 threat defense virtual . By default it has the following three key-value pairs to configure: • 'admin' user password • management center virtual hostname • the management center virtual hostname or CSF-DM for management. 'ManageLocally : yes' - This configures the CSF-DM to be used as threat defense virtual manager. You can configure the management center virtual as threat defense virtual manager and also give the inputs for fields required to configure the same on management center virtual.

Parameter Name	Examples of allowed Values/Type	Description
virtualNetworkResourceGroup	cisco-tdv-rg	Name of the resource group containing the virtual network. In case virtualNetworkNewOrExisting 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'.
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'.

Parameter Name	Examples of allowed Values/Type	Description
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.
vmSize	Standard_D4_v2	Size of the threat defense virtual VM. Standard_D3_v2 is the default.

Step 7 Use the ARM template to deploy 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 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 threat defense virtualthreat defense virtualthreat defense virtualthreat 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 threat defense virtual images using a compressed VHD image available from Cisco. This process is similar to deploying 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 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 threat defense virtual .

Procedure

Step 1 Download the 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 threat defense virtual parameter file. See the sample for the Azure 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 threat defense virtual deployment:

Parameter Name	Examples of allowed values/types	Description
vmName	csf-tdv	Name the 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 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.

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).
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\" :\"cisco-tdv\", \"ManageLocally\":\"No\", \"IPv6Mode\": \"DHCP\"}`	The field to provide in the Day 0 configuration to the threat defense 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 threat defense virtual manager. You can configure the CSF-MCv as 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

Parameter Name	Examples of allowed values/types	Description
		'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 '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

Parameter Name	Examples of allowed values/types	Description
		'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 threat defense virtual VM. Standard_D3_v2 is the default.

Step 4 Use the ARM template to deploy 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 threat defense virtual's IP configuration in Azure.

Threat Defense Virtual Image Snapshot

You can create and deploy the threat defense virtual using a snapshot image in the Azure portal. The image snapshot is a replicated threat defense virtual image instance with no state data.

Threat Defense Virtual Snapshot Overview

The process of creating a snapshot image of the threat defense virtual instance helps to minimize the initial system *init* time by skipping the first boot procedures done for the threat defense virtual and FSIC. The snapshot image consists of prepopulated database and the 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 management center or any other management center. This process helps in faster boot time of threat defense virtual, which is essential in auto scale deployment.

Create the Threat Defense Virtual Snapshot Image from Managed Image

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

Before you begin

You must have created a managed image of the 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 16.

You must not register the threat defense virtual instance you are preparing for image snapshot to any manager such as the management center or the device manager.

Procedure

Step 1 Go to Azure portal where you have created the managed image of the threat defense virtual instance.

Note
Ensure that the threat defense virtual instance which you are planning to replicate is not registered to the management center or configured to any other local manager or applied with any configuration.

Step 2 Go to **Resource Group** and select the threat defense virtual instance.

Step 3 Click the **Serial Console** on the navigation page of the 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 threat defense virtual instance. After the processing is done, the 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 threat defense virtual instance.

Step 9 Click **Review+Create** to create a new snapshot image of the threat defense virtual instance.

What to do next

Deploy the threat defense virtual instance using snapshot image. See Deploy the Threat Defense Virtual Instance using Image Snapshot.

Deploy the Threat Defense Virtual Instance using Image Snapshot

Before you begin

Cisco recommends the following:

- Confirm that a snapshot image is available for the 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 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 threat defense virtual instance using the snapshot image. See Deploy from Azure Using a VHD and Resource Template, on page 16.

Note
You can run the CLI commands **show version** and **show snapshot detail** from the threat defense virtual console to know about the version and details of the newly deployed threat defense virtual instance.