FortiOS - VMware NSX-T Administration Guide

Version 6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 30, 2022
FortiOS 6.4 VMware NSX-T Administration Guide
01-643-688069-20220830

TABLE OF CONTENTS

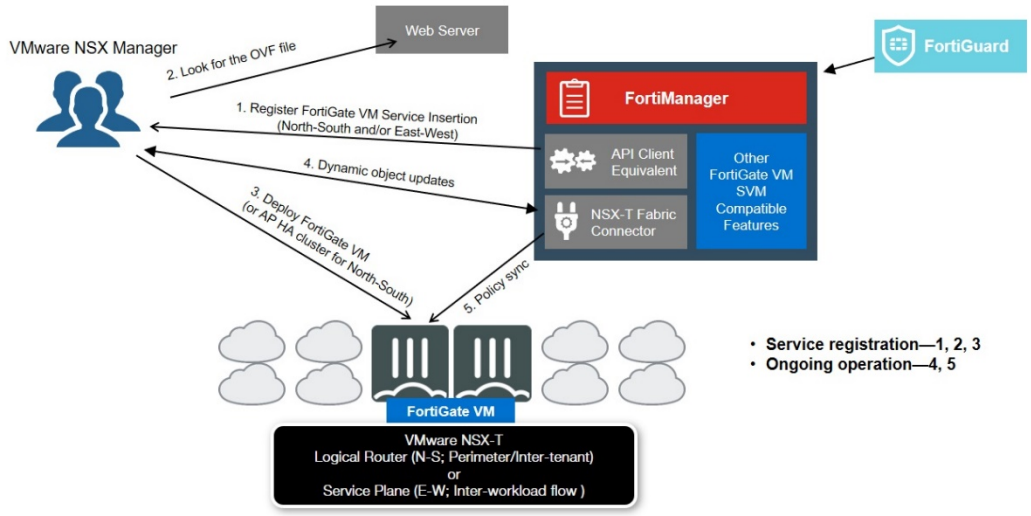
About FortiGate for VMware NSX-T

Fortinet's FortiGate-VM is a next generation firewall virtual appliance for VMware environments that provides purpose-built integration for VMware's Software-Defined Data Center (SDDC) and interoperability with NSX-T through service insertion as a third-party edge firewall. FortiGate-VM provides protection of north/south and east/west traffic flow inside the VMware NSX-T environment.

FortiGate-VM 6.4.3 is certified for a new deployment with NSX-3.0.0.1+ and 3.1.0+ as a firewall node for north-south edge service insertion or east-west service chaining. Upgrade to FortiOS 6.4.4 and later versions is supported.

NSX-T fully supports ESXi and KVM as hypervisor platforms. Only ESXi only (not KVM) supports an edge firewall, meaning that you need FortiGate-VM deployment images for ESXi.

The VMware-certified Fortinet solution requires a paired deployment of FortiManager (physical appliance or VM) and FortiGate-VM. Use supported versions for both products to integrate to a specific NSX-T version. You can find supported version information in the *VMware Compatibility Guide*.



FortiGate-VM alone can work with NSX-T as a firewall node. However, FortiGate single product deployment has not been certified with NSX-T.

Limitations

FortiGate-VM has the following limitations:

Policies

IPv4 and IPv6 policies are visible in the GUI but are not used. Virtual wire pair policy is used to configure firewall policies in working with NSX-T. Usually you create and manage policies in FortiManager to centrally manage FortiGates, and you do not need to log in to each FortiGate unless intended.

Product evaluation

You can only evaluate the product without purchasing a valid license when using FortiGate-VM and FortiManager-VM.

A FortiGate-VM evaluation license activates FortiGate features with low encryption mode. You must manually set the FortiManager-VM to low encryption mode and its SSL protocol to use TLS 1.0 to work in conjunction with the FortiGate-VM low encryption mode. After the evaluation period ends, you can purchase and apply valid licenses on both the FortiGate-VM and FortiManager-VM. Their product serial numbers change when promoted from low encryption mode. Subsequently, you must reregister FortiGate-VMs on FortiManager as managed devices and reapply their policy packages.

This evaluation behavior applies to all cloud integrations, not just VMware NSX-T, when you evaluate FortiGate-VM and FortiManager-VM as a pair.

To set low encryption mode on the FortiManager-VM:

1. In the FortiManager CLI, Run the following commands:
```
config system global
   set ssl-low-encryption enable
   set ssl-protocol tlsv1.0
end
```
2. The browser resets. Run `show system global` to check that FortiManager applied the changes. The output should be as follows:
```
config system global
   set hostname "FortiManager"
   set ssl-low-encryption enable
   set ssl-protocol tlsv1.0
   set usg enable
end
```

Models

FortiGate-VM

FortiGate-VM is available with different CPU and RAM sizes.

Model name	vCPU		RAM minimum
	Minimum	Maximum	
FG-VM01 or 01v	1	1	2 GB
FG-VM02 or 02v	1	2	2 GB
FG-VM04 or 04v	1	4	2 GB
FG-VM08 or 08v	1	8	2 GB
FG-VM16 or 16v	1	16	2 GB
FG-VM32 or 32v	1	32	2 GB
FG-VMUL or ULv	1	Unlimited	2 GB

By default, the v-series does not support virtual domains (VDOMs). To run VDOMs on v-models, you must purchase additional VDOM licenses. You can add and stack VDOMs up to the maximum supported number after initial deployment.

The number of vCPUs and the RAM size that the license indicates do not restrict the FortiGate from working, regardless of how many vCPUs and how much RAM the virtual instance includes. However, only the licensed number of vCPUs and RAM size process traffic and management. The FortiGate-VM does not use the rest of the vCPUs.

Example for FGT-VM08 license, where max 8vCPU is consumable:

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	The FortiGate-VM uses 8 VCPUs for traffic and management and does not use the rest.	The FortiGate-VM uses 8 VCPUs for traffic and management and does not use the rest.

This example applies to the RAM size as well.

Evaluation licenses

By default, the FortiGate-VM virtual appliance includes a limited 15-day evaluation license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- Low encryption only (no HTTPS administrative access)
- All features except FortiGuard updates

By default, FortiManager-VM includes a full-featured 15-day evaluation license.

If you evaluate both FortiGate-VM and FortiManager-VM without their valid full licenses, configure FortiManager-VM in low encryption mode before managing FortiGate-VM. See Product evaluation on page 5.

Note the following:

- Attempting to upgrade the FortiGate firmware locks the GUI until you upload a full license.
- The evaluation license does not incldue technical support.
- The trial period begins the first time that you start the FortiGate-VM.
- After the trial license expires, functionality is disabled until you upload a full license file.

If you require evaluation licenses valid for longer periods, such as 60 days, contact your Fortinet reseller.

Certification information

The following summarizes FortiGate-VM 6.4 certification information on VMware NSX-T:

Version	VMware NSX-T version	Certification date	Validity	Listing
6.4.3	2.5, 3.0 and 3.1	November 2020	N/A	https://www.vmware.com/resources/compatibility/detail.php?productid=51464&deviceCategory=nsxt

Deploying FortiGate and FortiManager on VMware NSX-T

Preparing for deployment

VMware NSX-T 2.5, 3.0.0+, and 3.1.0+ environments support this deployment with FortiOS 6.4.3+ and FortiManager 6.4.5+. The document provides screenshots from VMware NSX-T 3.0.0+.

This guide assumes that you have addressed the following requirements:

Virtual environment

You have deployed hypervisors (ESXi/KVM) on physical servers as NSX-T requires, with sufficient resources to support the FortiManager, FortiGate-VM, and all other VMs that you will deploy on the platform. Ensure that you have configured VMware NSX-T with logical switches, logical routers, and other components to support operating the third party edge device (the FortiGate-VM) before creating the FortiGate-VM. The NSX-T configuration may differ depending on east-west or north-south topology use cases.

VMware vCenter is optional for NSX-T.

Internet connectivity

FortiManager requires an outgoing Internet connection to contact FortiGuard to validate Fortinet licenses. There is a typical network topology where FortiGate-VM nodes are in a closed environment for east-west, and thus they must be able to connect to a FortiManager to validate the FortiGate-VM license.

Do not allow anonymous access to FortiManager and FortiGate-VM as an edge firewall from other networks, including the Internet. By default, there is no login password for both following deployment.

Deployment prerequisites

You need the following before deploying FortiGate-VM:

- A web server (IIS, Apache, cloud storage, and so on) to host the FortiGate-VM's deployment files. The web server must have connectivity from NSX Manager and the API client below.
- FortiManager (physical or VM)
  - Connectivity to NSX Manager
  - Connectivity from/to FortiGate-VMs that you will deploy

Registering the FortiGate-VM

Registering the FortiGate-VM with Customer Service & Support allows you to obtain the FortiGate-VM license file.

To register the FortiGate-VM license:

1. Log in to the Customer Service & Support site using a support account, or select *Sign Up* to create an account.
2. Select *Asset*, then select *Register/Activate*.
3. In the *Registration* page, enter the registration code that you received via email, and select *Register* to access the registration form.
4. Complete and submit the registration form.
5. In the registration acknowledgment page, click the *License File Download* link.
6. Save the license file (.lic) to your local computer.
7. After registering a license, Fortinet servers may take up to 30 minutes to fully recognize the new license. When you upload the license (.lic) file to activate the FortiGate-VM, if you get an error that the license is invalid, wait 30 minutes, then try again.

Registering the FortiManager-VM requires a similar process to the FortiGate-VM. See Registering your FortiManager VM.

NSX-T deployment package contents

The FortiGate-VM virtual appliance deployment package contains the following components:

Component	Description
fortios.vmdk	FortiGate-VM system hard disk (root device) in VMDK format.
datadrive.vmdk	FortiGate-VM log disk (second drive) in VMDK format.
FortiGate-VM64-1CPU.nsxt.ovf	Single core Open Virtualization Format (OVF) template.
FortiGate-VM64-1CPU.nsxt.cert	Single core signature file.
FortiGate-VM64-1CPU.nsxt.mf	Single core file checksum.
FortiGate-VM64-2CPU.nsxt.ovf	Two core OVF template.
FortiGate-VM64-2CPU.nsxt.cert	Two core signature file.
FortiGate-VM64-2CPU.nsxt.mf	Two core file checksum.
FortiGate-VM64-4CPU.nsxt.ovf	Four core OVF template.
FortiGate-VM64-4CPU.nsxt.cert	Four core signature file.
FortiGate-VM64-4CPU.nsxt.mf	Four core file checksum.
FortiGate-VM64-8CPU.nsxt.ovf	Eight core OVF template.
FortiGate-VM64-8CPU.nsxt.cert	Eight core signature file.
FortiGate-VM64-8CPU.nsxt.mf	Eight core file checksum.

Place the FortiGate-VM deployment files on a web server and make them available for download. You can use any web server, such as Apache or IIS. Note the file location URL (HTTP or HTTPS).

Customizing the OVF file to change the number of vCPUs and size for the FortiGate-VM

You can customize the OVF file for deployments where you require more than eight vCPUs.

To customize the OVF file to change the number of vCPUs and size for the FortiGate-VM:

1. Open one of the OFV files from NSX-T deployment package contents on page 9 in a text editor.
2. Replace the value in lines 46 and 49 with the required core count.

```
43      <Item>
44        <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
45        <rasd:Description>Number of Virtual CPUs</rasd:Description>
46        <rasd:ElementName>8 virtual CPU(s)</rasd:ElementName>
47        <rasd:InstanceID>1</rasd:InstanceID>
48        <rasd:ResourceType>3</rasd:ResourceType>
49        <rasd:VirtualQuantity>8</rasd:VirtualQuantity>
50      </Item>
```

3. Modifying the core count or any variable in the OVF file causes the OVF integrity check with the manifest (.mf) to fail. You must disable strict certificate manifest check from the NSX-T Manager CLI:
   a. Log in or SSH to NSX-T Manager as root.
   b. Run the following:

```
sed -i
     's/set.vm.deployment.strict.cert.manifest.check=true/set.vm.deployment.strict.c
     ert.manifest.check=false/' /usr/tanuki/conf/cm-inventory-tomcat-wrapper.conf
```

   c. Restart the `cm-inventory` service:

```
service cm-inventory restart
```

You can customize the OVF to change the number of vCPUs and RAM size for the FortiGate-VM, then apply the corresponding VM license as Models on page 5 describes.

Deploying and connecting to the FortiManager

To deploy and connect to FortiManager:

1. Do one of the following:
   a. If you are deploying a FortiManager-VM, do the following:
      i. Deploy FortiManager-VM on ESXi, which is part of the NSX-T environment. For details on how to deploy the FortiManager-VM, see Deploying FortiManager VM on VMware vSphere.
      ii. After the FortiManager-VM deployment, log in to https://<FortiManager IP address> in your browser. Resetting the password at first login is strongly encouraged. Make the initial configuration and ensure connectivity between FortiManager and NSX Manager. For details on initial configuration, see Configuring initial settings.
      iii. Upload the valid license file and activate FortiManager. The system reboots. FortiGate-VM can connect to FortiManager.
   b. If you are using a FortiManager appliance, go to step 2.
2. Log in to FortiManager.
3. Enabling the multiple administrative domain (ADOM) feature is recommended for ease of administration. Create a new ADOM or select an existing one for deployment. In FortiManager 6.4, you can create multiple connectors per ADOM and multiple service definitions per connector. You cannot specify the same NSX Manager in multiple

ADOMs. See Administrative Domains.
If you create an NSX service definition in the root ADOM, ensure that the root ADOM version is 6.4.
VMs deployed via the NSX-T Manager must be in the same ADOM that their respective connectors are created in and cannot be moved.

Automatically downloading the FortiGate-VM license

FortiGate-VMs deployed via FortiManager can download licenses directly from an HTTP(S) server. For this functionality, you must adhere to the following naming convention.

To automatically download the FortiGate-VM license:

1. Rename the license file with the FortiGate-VM management IP address in the format <FortiGate management IP address>.lic. For example, if the IP address is 10.1.20.20, rename the license file 10.1.20.20.lic.
   For North-South deployments, you can manually assign the FortiGate-VM management IP address. Administrators should plan the management plane with the license naming convention in mind.
   For East-West deployments, you can configure FortiGate-VM management IP address via DHCP or NSX-T IP address pools. Using NSX-T IP pools is recommended as it simplifies administration tasks. Ensure that the number of IP addresses in the pool is the same as the number of FortiGate-VMs to deploy. Ensure that you have renamed licenses using the convention described.
2. Store the license file on an HTTP(S) server that the FortiGate-VM can reach. For East-West deployments, ensure that you have stored enough licenses for the desired number of FortiGate-VMs to deploy.
3. Note the URL of the directory where you store the file.

Registering the service insertion definition to NSX-T

With the NSX-T integration, you can register to the partner service catalog through FortiManager to NSX Manager. This step applies commonly to FortiManager-VM and FortiManager physical appliances.

To register the service insertion definition to NSX-T:

1. Log in to FortiManager, then select the desired ADOM.
2. Go to *Fabric View* > *Fabric Connectors*.
3. Click *Create New* > *VMware NSX-T*.
4. In the *Create New Fabric Connector* page, fill out the following fields:

Name	Enter a unique name to identify the NSX-T Connector.
Status	Keep the status *OFF* until you have configured the other fields.
NSX-T Manager Configurations	
Server	Enter the NSX-T Manager IP address.
User Name	Enter the username to access the NSX-T Manager.

Password	Enter the password.
FortiManager Configurations	
IP Address	Enter the FortiManager IP address. Usually it is the same IP address that you are accessing in the browser.
User Name	Enter the username to access the FortiManager.
Password	Enter the password.

5. Click *OK* to save the changes. Then, toggle the *Status* to *ON*.
6. Add the service:
   a. Open the newly created NSX-T Connector. Under *Registered Services*, click *Add Service*.
   b. In the *Service Name* field, enter the service name to register under to NSX-T's partner service catalog.
   c. For *Integration*, select *East-West* or *North-South* as desired.
   d. In earlier steps, you placed FortiGate-VM deployment image files on a web server. In the *Image Location* field, enter the file location URL in the format http://<IP address of web server>/<directory>/FortiGate-VM64.nsxt.ovf.
   e. Enter the URL of the directory containing the license files in the *License URL Prefix*. This directory should contain the license file, OVF, and both VMDK files. The FortiGate-VM automatically downloads the license and validates it on bootup. If license validation fails, you can upload a new valid license via the FortiOS UI. The FortiGate must have a valid license before connecting to FortiManager.
   f. From the *Type* dropdown list, select the desired SKU. This does not have any bearing on the SKU of the FortiGate-VM being deployed, as the OVF file configuration determines this. However, this can be useful in letting the user know which SKU is configured to be deployed on the NSX Manager UI. You can specify multiple SKUs in the service field in FortiManager. You can use this to upgrade or downgrade the deployment via NSX-T when required.

You now see the service registered with NSX-T. After waiting a few minutes, if FortiManager connects to NSX-T, it populates the dynamic address objects as you can see in FortiManager configurations and NSX-T's inventory groups. You can use the objects to configure firewall policies.

To ensure automatic dynamic address population, execute the following CLI command in the FortiManager CLI:

```
config system admin user
   edit <admin (username specified in FortiManager connector
        configuration)>
      set rpc-permit read-write
   next
end
```

Lack of read-write permissions on `rpc-permit` causes dynamic addresses to not be automatically populated.

Removing an NSX-T connector

If you no longer need the NSX-T connector configuration, you can remove it.

To remove an NSX-T connector:

1. In FortiManager, go to *Fabric View* in the desired ADOM.
2. Edit the desired NSX-T connector configuration.
3. Click *Disable Server*, then click *OK* to confirm. If the server does not become disabled, delete any service deployments deployed as part of this connector on the NSX-T Manager, then try to disable it again.
4. Ensure the *Status* is *OFF*. If it is *ON*, toggle the *Status* to *OFF* and click *Apply & Refresh* or *OK*.
5. Return to *Fabric View*. Right-click the NSX-T connector, then click *Delete*.

Deploying the FortiGate-VM on NSX-T

After you deploy FortiManager and configure it to register services on NSX-T, you can deploy FortiGate-VM on the NSX-T management console.

To deploy the FortiGate-VM on NSX-T:

1. Log in to NSX-T Manager.
2. Go to *System* > *Service Deployments* > *Configuration)* > *Deployment*.
3. Select the service definition that you just registered through FortiManager in the *Partner Service* dropdown list.
4. Click *DEPLOY SERVICE*.
5. Do one of the following:
   a. For North-South deployments, populate the attachment points, compute manager, cluster, and datastore as required. Click *SAVE*.
   b. For East-West deployments, populate the attachment points, compute manager, cluster, and datastore as required. From the *Deployment type* dropdown list, select *Host based* or *Clustered*. Uplink connection is defined in the Service Segments section. See Add a Service Segment. Click *SAVE*.
6. Configure the networks:
   a. For North-South deployments, set static network configuration for only the management IP address port1 (eth0). eth1 is mapped to port2. eth3 is mapped to port3. This operates as virtual wire pair to handle traffic. eth3 is mapped to port4 if you want to configure two FortiGate-VM nodes to form an active-passive high availability (HA) cluster. This will be the HA heartbeat. NSX-T only allows North-South deployments to have A-P HA. If you set the *Deployment Mode* field to standalone, interface eth3 is unused. Assigning static IP addresses to all interfaces is recommended in case you want to configure HA in the future.
   b. For East-West deployments, you only need to configure network configuration for the management IP address port1 (eth0). You can set the management IP address via DHCP or NSX-T IP address pools. Using NSX-T IP address pools is recommended for easier administration. See Create an IP Pool in Manager Mode. eth1 mapped to port2 is split into two virtual interfaces and operated as a virtual wire pair to handle traffic. This is not user-configurable.
   c. Click *SAVE* in the *Networks* dialog.
7. Click *SAVE* in the *DEPLOY SERVICE* dialog to initiate deployment. A few minutes later, the service and service instance appear in the *DEPLOYMENT* and *SERVICE INSTANCES* tab, respectively.

Connecting to the FortiGate-VM

1. In a browser, go to <http://FortiGate-VM IP address>. This is the generally preferred method. After the FortiGate-VM becomes licensed, you can go to <https://IP address>.
2. Select the login access level.
3. After logging in, you can change the default hostname and registration with FortiCare support. Click *Later*. You should only change the password in FortiManager to avoid synchronization issues.
4. The FortiGate-VM dashboard displays. If the license file that you provided in Deploying the FortiGate-VM on NSX-T on page 13 was invalid, go to *System* > *FortiGuard* > *FortiGate VM License* to uploada valid license.

Managing FortiGate-VM on FortiManager

After deploying the FortiGate-VM, you must register it as a managed device on FortiManager. FortiManager eases management, especially when you have multiple FortiGate-VM nodes, by providing a single pane of glass and allowing you to centrally manage firewall policies.

The steps described apply commonly to FortiManager-VM and FortiManager physical appliances.

Newly added devices are listed in the root ADOM under Device Manager as unauthorized.

To manage FortiGate-VM on FortiManager:

1. Log in to FortiManager and enter the root ADOM.
2. Go to *Device Manager*.
3. Under *UnAuthorized Devices*, select the newly installed FortiGate-VM.
4. Click *Authorize device*.
5. Select the ADOM that you want to add the device to. Adding the VM to the same ADOM as the NSX-T connector is recommended.
6. After FortiManager authorizes the device, click the FortiGate-VM and select *Import Policy*.
7. For *Object Selection*, ensure that *Import all objects is selected* to ensure that FortiManager imports the virtual wire pair. Click *Next*.
8. Do not modify external and internal under *ADOM Interface*. Click *Next*.
9. You have successfully registered the FortiGate-VM as managed device under Managed Devices. Check the configuration:
   a. Double-click the device name to show the FortiGate-VM dashboard.
   b. Under *Policy Package Status*, click the policy package name. FortiManager displays the Policy Packages page.
   c. Click *Tools* > *Display Options*.
   d. Ensure that *Virtual Wire Pair Policy* is enabled, then click *OK*. Virtual wire pair policy is the firewall policy package to use for the FortiGate-VM, which works as service insertion/chaining on NSX-T. The policy list in the left pane displays the IPv4 virtual wire pair policy. The right pane may be empty at this step.

Creating an address

Before applying firewall policies to the FortiGate-VM, you must create addresses to apply as sources or destinations in the policies. This example creates an address based on the dynamic address objects that have been populated from NSX-T's Inventory through the NSX-T Connector.

To create an address:

1. In FortiManager, go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*. Click *Create New* > *Address*
2. Configure the address as follows:

Address Name	Enter a unique name.
Type	Select *Dynamic*.
Sub Type	Select *FSSO*.
FSSO Group	Select the desired dynamic objects from the *Select Entries* dialog. This assumes that you already have inventory groups on NSX-T. Click *OK*.
Per-Device Mapping	Optionally, you can add particular FortiGate-VM devices.

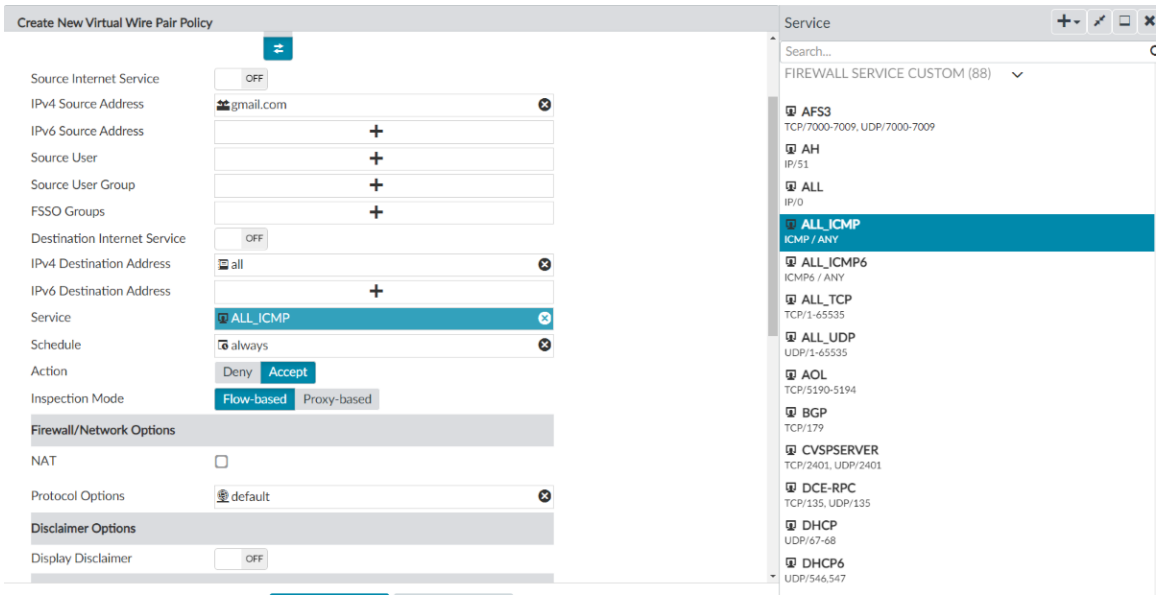
3. Click *OK*. FortiManager creates the address.

Managing firewall policies

To create and configure a firewall policy:

1. In FortiManager, go to *Policy & Objects* > *Policy Packages* > *<desired policy package>* > *Virtual Wire Pair Policy*.
2. Click *Create New* or double-click an existing policy that FortiManager imported from the FortiGate-VM.
3. Configure the policy:
   a. In the *Name* field, enter the policy name.
   b. In the *Virtual Wire Pair* field, select the bidirectional option.
   c. For *Source Address* or *Destination Address*, select a previously created address.

d. For *Service*, specify a protocol to apply. This example selects ICMP.



e. For *Action*, select *Accept*.

f. Select between *Flow* and *Proxy*-based inspection modes.

g. Under *Firewall/Network Options*, configure NAT with IPv4/IPv6 dynamic IP address pools if needed.

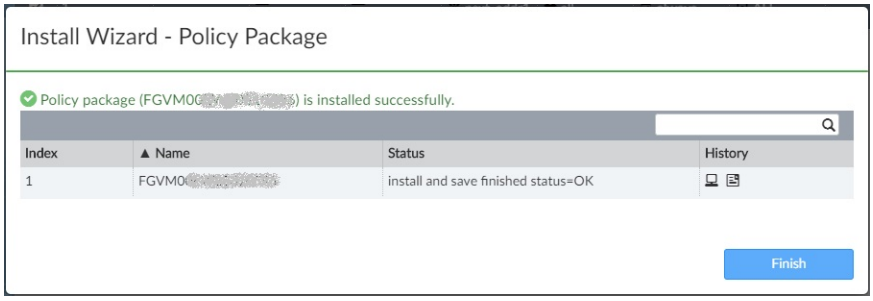
h. Under *Disclaimer Options*, display customized messages for certain actions.

i. Under *Security Profiles*, for SSL/SSH inspection, choose the desired packet inspection level.

j. Under *Traffic Shaping Options*, set traffic priorities to ease network congestion.

k. To log traffic, enable *Log Security Events* or *Log All Sessions*. You can capture packets with these options, which helps with troubleshooting. Click *OK*.

4. Create other firewall policies as desired. This example has one policy that allows ICMP bidirectionally between the specified sources and destinations, and denies all other traffic.
5. Push the policy package to the FortiGate-VM:
   a. Right-click the policy package that contains the firewall policies to apply to the FortiGate-VM, then click *Install Wizard*.
   b. Select the FortiGate-VMs where you applied the policy package, then click *Next*.
   c. After FortiManager applies the package, click *Finish*. FortiManager has now installed the policy package. The FortiGate-VM now has the policy synchronized with FortiManager.



6. Ping from a source to destination to verify that it goes through and to verify that all other traffic does not go through the FortiGate-VM.

Configuring a redirection policy

You must configure a redirection policy on NSX-T.

For an east-west topology, complete the following steps for Service Insertion for East-West Traffic:

- Add a Service Profile
- Add a Service Chain
- Add Redirection Rules for East-WestTraffic

For a north-south topology, configure traffic redirection.

Associating an NSX-T service profile with a VDOM

You can associate NSX-T service profiles with individual VDOMs of FortiGate instances to redirect traffic from one VDOM to another.

To associate an NSX-T service profile with a VDOM:

1. Create a service profile for each VDOM in the VMware NSX-T:
   a. Go to *Security* > *Settings (Network Introspection Settings)* > *Service Profiles*.
   b. Click *ADD SERVICE PROFILE*.
   c. In the *Service Profile Name* field, enter the desired name.
   d. From the *Vendor Template* dropdown list, select the desired template.
   e. Click *SAVE*.
   f. Repeat the process for other VDOMs as desired.
2. Create a service chain for each VDOM:
   a. Go to *Security* > *Settings (Network Introspection Settings)* > *Service Chains*.
   b. Click *ADD CHAIN*.
   c. In the *Name* field, enter the desired name.
   d. From the Service Segments dropdown list, select the desired service segment.
   e. In the *Forward Path* field, add the service profile that you created in step 1.
   f. Add other service profiles in sequence as needed.
   g. Enable *Inverse Forward Path*.
   h. Click *SAVE*.
3. Configure the NSX-T connector:
   a. In FortiManager in the same ADOM as the NSX-T connector, go to *Policy & Objects* > *Object Configurations* > *Endpoint/Identity*.
   b. Select the NSX-T connector, then click *Configure*.
   c. Select a service, then click *Configure*.
   d. Click *Add* to add a new service chain.
   e. From the *Device* dropdown list, select the device to which to apply the service chain.
   f. From the *Index* and *Reverse Index* dropdown lists, select the newly created service profile.
   g. From the *Chain ID* and *VDOM* dropdown lists, select the chain ID and VDOM to apply the service chain to.
   h. Click *OK*.

4. Import the device settings to the FortiGate:
   a. In FortiManager, go to *Device Manager*.
   b. Select the FortiGate to apply the newly created policy to.
   c. Run the install wizard to import the changed device settings.
5. In NSX-T Manager, go to *Security* > *Network Introspection (E-W)*.
6. Click *ADD POLICY*.
7. Select the chain that corresponds to the VDOM where traffic will be redirected.
8. In the policy options menu, click *Add Rule* to add the new rule to the policy.

NSX-T allows you to create rules that apply to the same security group under different policies. See Add Redirection rules for E-W traffic. This configuration is not recommended while using VDOMs, as it may lead to unintended behavior.

See East-West Network Security - Chaining Third-party Services for information on configuring redirection rules.

9. Click *Publish* to apply changes.

Liveness detection

Liveness detection can force the service insertion datapath not to use a specific VM until its service manager has updated the VM configuration. This can be required when a new FortiGate-VM is deployed and should not reply to liveness detection queries or forward any traffic until it has received the required configuration from the service manager or during maintenance of said VM. The service insertion platform instead uses an already configured VM if one is available.

NSX-T 2.5 and later versions support this feature. See VMware NSX-T documentation.

When configuring a service from FortiManager to VMware NSX-T, the option to enable or disable liveness detection is available. By default, liveness detection is disabled.

To configure NSX-T service with liveness detection:

1. Create a service chain and profile in VMware NSX-T as Add Service Profile and Add Service Chain describe. When creating the service chain, in the *Failure Policy* field, set *Allow* to redirect traffic to the destination VM when the service VM fails.
2. Add a service chain and configure liveness detection in FortiManager:
   a. Go to *Policy & Objects* > *Object Configurations* > *Endpoint/Identity*.
   b. Select the NSX-T connector, then click *Configure*.
   c. Click *Add* to add a new service chain.
   d. From the *Device* dropdown list, select the required VM or FortiGate.
   e. Ensure that *Enable Liveness Detection* is set to *ON*. It is enabled by default.
   f. Configure other fields as required.
   g. Click *OK*.

3. In FortiManager, verify if liveness detection is enabled:
   a. Go to Policy & Objects > Object Configurations > Endpoint/Identity.
   b. Select the added NSX-T service, then click Configure.
   c. Select a service, then click Configure. FortiManager displays a list of all service chains with a Liveness Detection column.

Liveness detection is a global setting for a FortiGate instance. If enabled, it applies across all VDOMs in the FortiGate.

4. Import the device settings to the FortiGate:In FortiManager, go to *Device Manager*.Select the FortiGate to apply the newly created policy to.Run the install wizard to import the changed device settings.

SDN connector integration with VMware NSX-T

See the *FortiOS Administration Guide*.

Change log

Date	Change Description
2021-02-22	Initial release.
2022-08-30	Added Certification information on page 6.