Nutanix Administration Guide

FortiOS 7.2

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

March 31, 2022
FortiOS 7.2 Nutanix Administration Guide
01-720-793065-20220331

TABLE OF CONTENTS

Deploying FortiGate-VM on Nutanix

Obtaining the deployment image

To obtain the deployment image:

1. Go to Customer Service & Support and log in.
2. Go to *Support* > *VM Images*.
3. From the *Select Product* dropdown list, select *FortiGate*.
4. From the *Select Platform* dropdown list, select *KVM*.
5. Download the deployment package file (FGT_VM64_KVM-v7.2.x-buildXXXX-FORTINET.out.kvm.zip).

Uploading the FortiGate deployment image to Nutanix

To upload the FortiGate deployment image to Nutanix:

1. Log in to the Nutanix Prism Central console.
2. Upload the FortiGate-VM image:
   a. From the top-left corner, go to *Virtual Infrastructure* > *Images*.
   b. Click *Add Image*.
   c. Under *Image Source*, click *Image File*.
   d. In the *Add Images* window, click *Add File*.
   e. Select the VM image file downloaded in Obtaining the deployment image on page 4.
   f. In the *IMAGE TYPE* dropdown list, ensure *Disk* is selected.
   g. In the *IMAGE DESCRIPTION* field, enter the desired description.
   h. In the *Placement Method* and *Select Cluster* fields, specify settings as desired.
   i. Click *Save*.
   j. Wait a few minutes, then refresh the browser. You will find the newly created VM image in the image list.

Creating the FortiGate-VM from the image file

To create the FortiGate-VM from the image file:

1. In the Nutanix Prism Element console, go to the dashboard, then select *Create VM*.
2. Enter the following configuration information for *General Configuration* and *Compute Details*:
   a. In the *NAME* field, enter the desired name for your VM.
   b. Set the timezone.
   c. In the *VCPU(S)* field, enter the desired number.
   d. In the *MEMORY* field, enter the desired size. There are no RAM restrictions.
3. By default, a CD-ROM is listed under *Disks*. Delete the CD-ROM.
4. You must create a boot disk and a log disk for the VM. Create the boot disk:
   a. Click *Add New Disk*.
   b. The boot disk will be cloned from the VM image that you uploaded. Under *OPERATION*, select *Clone from Image Service*.
   c. Under *BUS TYPE*, select *SCSI*.
   d. Under *IMAGE*, select the FortiGate disk image.
   e. Click *Add*. The boot disk has been added.
5. Create the log disk:
   a. Click *Add New Disk*.
   b. Under *OPERATION*, select *Allocate on Storage Container*
   c. Select the desired *Bus Type* (for example, SCSI) and *Storage Container*.
   d. Under *SIZE (GB)*, enter *30*.
   e. Click *Add*. The log disk has been added.
6. Add a network interface for the VM:
   a. Double-click the FortiGate-VM in the VM list.
   b. Under *Network Adapters (NIC)*, click *Add New NIC*.
   c. Under *VLAN NAME*, select the desired VLAN. You can select DHCP fist to check connectivity. Changing the VLAN to a static IP address at a later time is recommended.
   d. Click *Add*.
7. Pin the VM to a host:
   a. In the VM configuration, under *VM Host Affinity*, click *Set Affinity*.
   b. Under *SELECT HOSTS*, select the desired host.
   c. Click *Save*.
8. Click *Save*. The system displays a *Successfully submitted Create operation* message when the VM has been created successfully with no error.

Registering and downloading your license

You can obtain licenses for the bring your own license (BYOL) licensing model through any Fortinet partner. If you do not have a partner, contact Fortinet for assistance in purchasing a license.

After you purchase a license or obtain an evaluation license (60-day term), you receive a PDF with an activation code.

To register and download your license:

1. Go to Customer Service & Support and create a new account or log in with an existing account.
2. Go to *Register Now* to start the registration process. In the *Registration Code* field, enter your license activation code and select *Next* to continue registering the product. Enter your details in the other fields.
3. At the end of the registration process, download the license (.lic) file to your computer. You will upload this license later to activate the FortiGate-VM.
   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 and try again.

Connecting to the FortiGate-VM

To connect to the FortiGate-VM:

1. Power on the VM:
   a. In Prism Element, find the newly created FortiGate-VM and go to its VM dashboard.
   b. By default, the FortiGate-VM is shutdown after initial creation. Click *Power On*. After a successful bootup, the FortiGate-VM instance now shows a green light.
2. Check the IP address on the *VM NICs* tab.
3. Access the FortiGate in your browser by going to https://<IP address>.
4. Log in to the FortiGate-VM with the username *admin* and no password.
5. After logging in successfully, upload your license (.lic) file to activate the FortiGate-VM. The FortiGate-VM automatically restarts. After it restarts, wait about 30 minutes until the license is fully registered at Fortinet, then log in again.

Configuring the second NIC

To configure the second NIC:

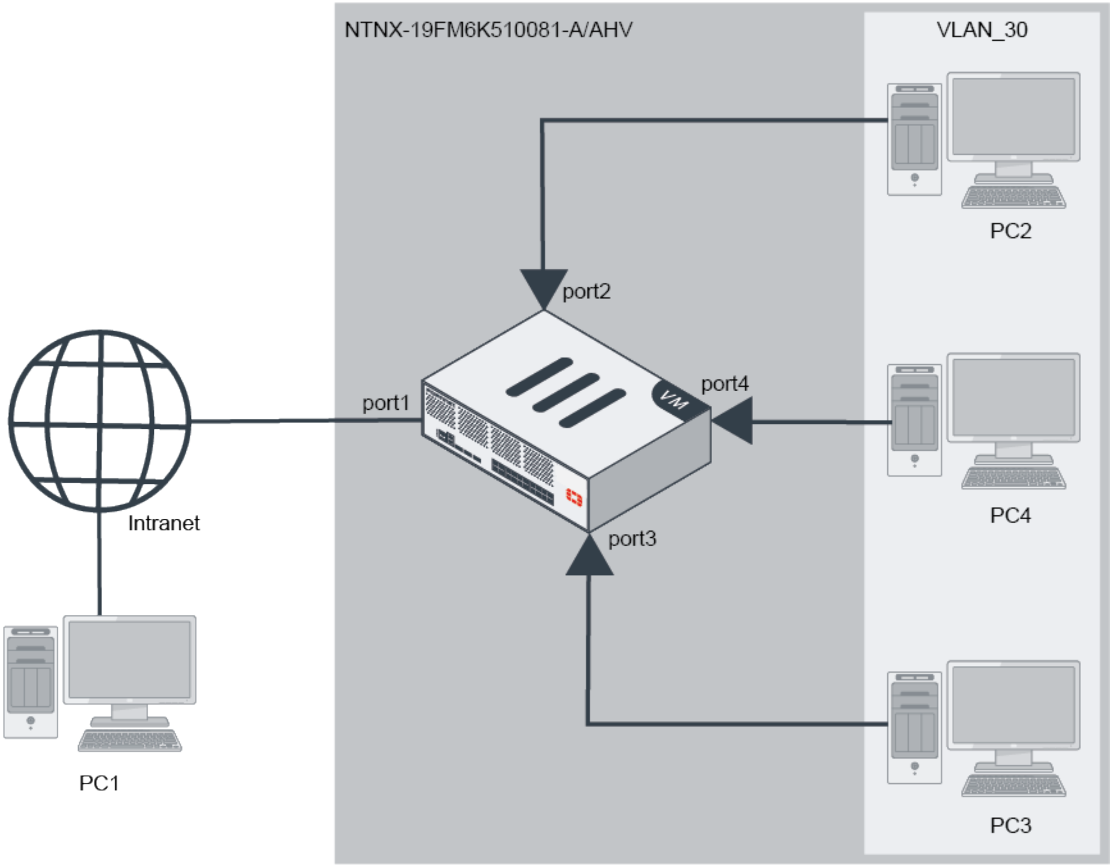
1. In Prism Element, find the FortiGate-VM and go to its VM dashboard.
2. Double-click the FortiGate-VM in the VM list, or click *Update*.
3. Under *Network Adapters (NIC)*, click *Add New NIC*.
4. From the *VLAN NAME* dropdown list, select the desired VLAN.
5. Click *Add*.
6. Click *Save*.
7. In your browser, log in to the FortiOS GUI.
8. Go to *Network > Interfaces*. The second NIC has been added, with no need to reboot the FortiGate.
9. Edit port2. Enter the IP address and netmask. Configure the other elements as needed, then click *OK*.

Deploying FortiGate-VM for service chaining

FortiOS supports Nutanix service chaining to allow a service chain to direct network traffic to the FortiGate-VM for scanning. This requires the Calm and Flow features to be enabled on Nutanix, and for Prism Central to be installed on the Nutanix Acropolis hypervisor (AHV).

Nutanix service chains define a set of network function VMs (NFV) for advanced traffic processing. You can direct each defined flow in an application policy through a service chain when a chain exists. For examples, the service chain can direct network traffic on a specific port to a VM for antivirus scanning, deep packet, inspection, or packet capture. You can combine NFVs in a chain to apply multiple functions to guest VM traffic.

The following shows an example topology for this feature:



The following describes the topology in this example:

- The Nutanix AHV has Prism Central installed, with Calm and Flow enabled.
- There are three Ubuntu VMs (PC2, PC3, and PC4) installed to AHV and connected to vlan30.
- The FortiGate-VM has the following interfaces attached:
  - One management interface
  - Three network function chain interfaces

With this topology, you can test whether the feature is functioning by directing traffic between PC2 and PC3 through the FortiGate's virtual wire pair port2-port3 interfaces by the Nutanix service chain feature.

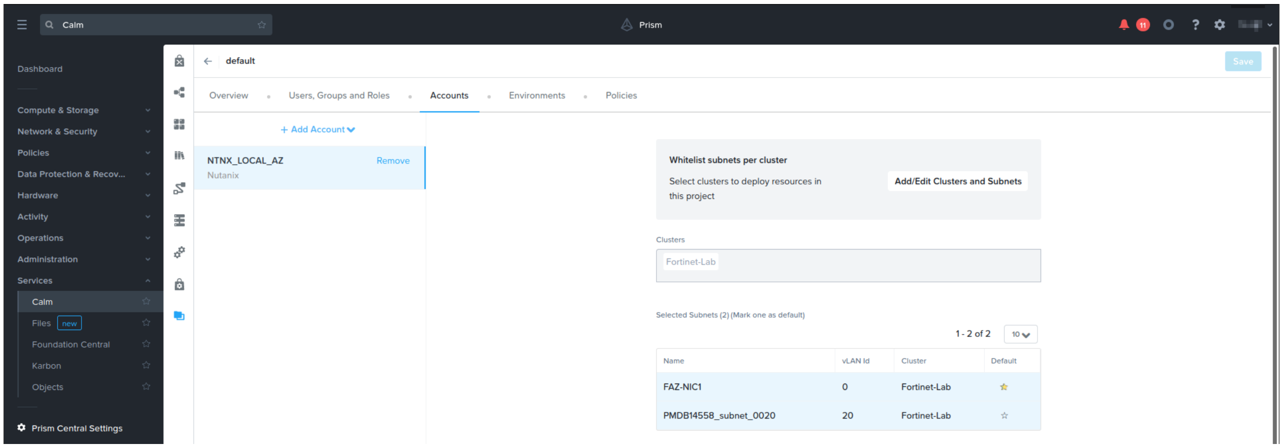
The following instructions describe how to configure the deployment that the topology diagram shows. Substitute the values from your own deployment where necessary.

These deployment instructions were tested using the following Nutanix platform details:

- Prism Central pc.2021.9.0.2
- Acropolis operating system 5.20.1.1
- Calm 3.3.0
- Cluster Maintenance Utilities 1.0.0.
- Epsilon 3.3.0
- Flow Security 1.0.0
- Licensing LM.2021.2.1
- NCC 4.3.0

To deploy the FortiGate-VM to the Nutanix cluster using the Calm blueprint:

1. Sign in to Prism Central.
2. Go to *Compute & Storage* > *Images*. Click *Import Images*, and upload the fortios.qcow2 image.
3. Go to *Services* > *Calm* > *Projects*. Add a user account to NTNX_LOCAL_AZ, selecting a default subnet.



NTNX_LOCAL_AZ
Nutanix

Whitelist subnets per cluster

Select clusters to deploy resources in this project

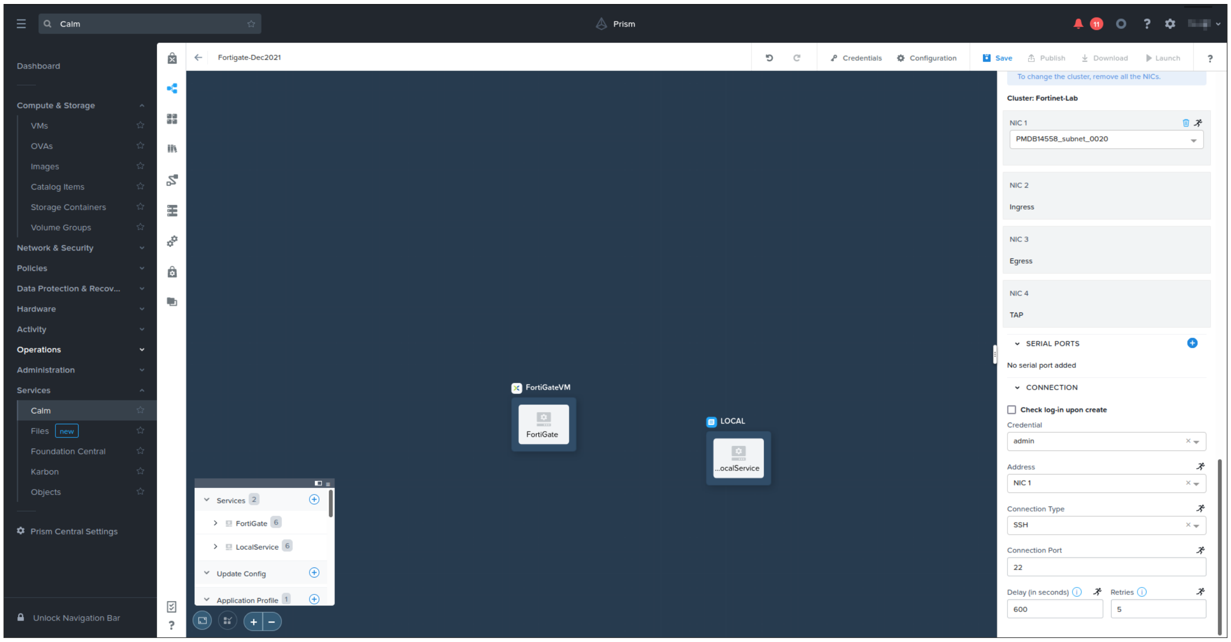
Clusters: Fortinet-Lab

Selected Subnets (2) (Mark one as default)

Name	vLAN Id	Cluster	Default
FAZ-NIC1	0	Fortinet-Lab	★
PMDB14558_subnet_0020	20	Fortinet-Lab	☆

4. Upload and configure the JSON file:
   a. Go to *Blueprint*. Upload the JSON file. In this example, it is Fortigate-Dec2021.json file.
   b. Go to *Credentials*, and set a password for the admin user. Save.
   c. Click the AHV application profile and configure it as follows:
      i. For *NF_CHAIN_NAME*, enter the desired chain name. In this example, it is FORTIGATE_CHAIN.
      ii. For *CLUSTER_NAME*, enter the desired cluster name. In this example, it is Fortinet-Lab.
      iii. For *PC_IP*, enter the PC IP address. In this example, it is 192.168.20.58.
5. Click *Services, Fortigate* to configure the VM name, operating system image, and network adapters:
   a. You will use a cloud-init script to configure the FortiGate-VM. Enable *Guest Customization*, and select *Cloud-init*. Enter the desired script.
   b. Under *Disks*, from the *Operation* dropdown list, select *Clone from Image Service*.
   c. From the *Image* dropdown list, select the fortios.qcow2 image.
   d. Connect NIC1 to the management subnet, and add three network function chain interfaces: NIC2 for ingress,

NIC2 for egress, and NIC4 for TAP.



To change the cluster, remove all the NICs.

Cluster: Fortinet-Lab

NIC 1: PMDB14558_subnet_0020

NIC 2: Ingress

NIC 3: Egress

NIC 4: TAP

SERIAL PORTS

No serial port added

CONNECTION

□ Check log-in upon create

Credential: admin

Address: NIC 1

Connection Type: SSH

Connection Port: 22

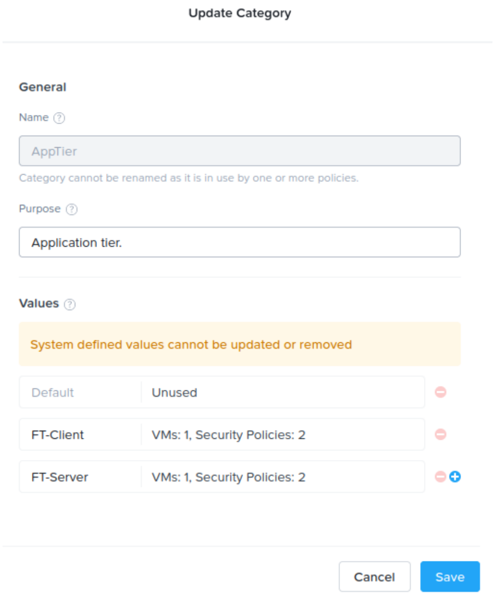
Delay (in seconds): 600

Retries: 5

6. Click *Save*.
7. Click *Launch*. In the *Application Name* field, enter the desired name to deploy the blueprint. In this example, it is Fortigate-BP.
8. Confirm that the resources were successfully deployed:
   a. Go to *Services* > *Calm* > *Applications*, and click the application name. In this example, it is Fortigate-BP.
   b. On the *Audit* tab, check the process status. The process may take ten to fifteen minutes. If an *IP not found error* occurs, disregard it. You can configure the port1 static IP address later through FortGate-VM console access.
   c. On the *Overview* tab, check the application summary.
   d. Go to *Administration* > *Categories*. Verify that the network_function_provider FORTIGATE_CHAIN was created.
9. Go to *Compute & Storage* > *VMs*. On the *List* tab, verify that the FortiGate-VM was deployed to AHV as NFVM. Select it, then select *Launch console*.

To direct traffic through the FortiGate-VM:

1. In Prism Central, go to *Categories* > *AppTier*. Click *Update*. Add FT-Client and FT-Server, then save.



Update Category

General

Name

AppTier

Category cannot be renamed as it is in use by one or more policies.

Purpose

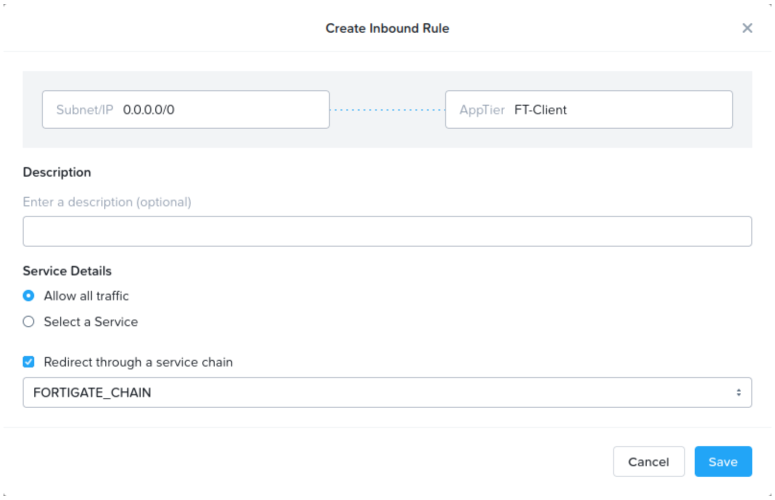
Application tier.

Values

System defined values cannot be updated or removed

Default	Unused
FT-Client	VMs: 1, Security Policies: 2
FT-Server	VMs: 1, Security Policies: 2

2. Go to *Categories* > *AppType*. Click *Update*. Add FT_AppType, then save.
3. Go to *Compute & Storage* > *VMs*. Right-click PC2. Select *Manage Categories*, then set the categories as follows:
   a. For *Environment*, select *Testing*.
   b. For *AppType*, select *FT_AppType*.
   c. For *AppTier*, select *FT-Client*.
4. Go to *Compute & Storage* > *VMs*. Right-click PC3. Select *Manage Categories*, then set the categories as follows:
   a. For *Environment*, select *Testing*.
   b. For *AppType*, select *FT_AppType*.
   c. For *AppTier*, select *FT-Server*.
5. Configure a security policy:
   a. Go to *Network & Security* > *Security Policies*. Click *Create Security Policy*, then click *Create*.
   b. In the *Name* field, enter the desired policy name. In this example, it is FT-Sec_policy.
   c. In the *Purpose* field, enter the desired purpose. In this example, it is testing.
   d. In the *Secure This App* field, select *FT_AppType*.
   e. Under *Inbounds*, in the *Add source by: Subnet/IP* field, enter 0.0.0.0/0. Click *Add*.
   f. Under *Outbounds*, in the *Add source by: Subnet/IP* field, enter 0.0.0.0/0. Click *Add*.
   g. Under *AppType FT_AppType*, select *Set rules on App Tiers, instead*. Add *AppTier: FT-Client*, and *FT-Server*.
   h. Configure the rules:
      i. For AppTier: FT-Client, create an inbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.



Create Inbound Rule

Subnet/IP 0.0.0.0/0

AppTier FT-Client

Description

Enter a description (optional)

Service Details

● Allow all traffic

○ Select a Service

☑ Redirect through a service chain

FORTIGATE_CHAIN

ii. For AppTier: FT-Server, create an inbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.

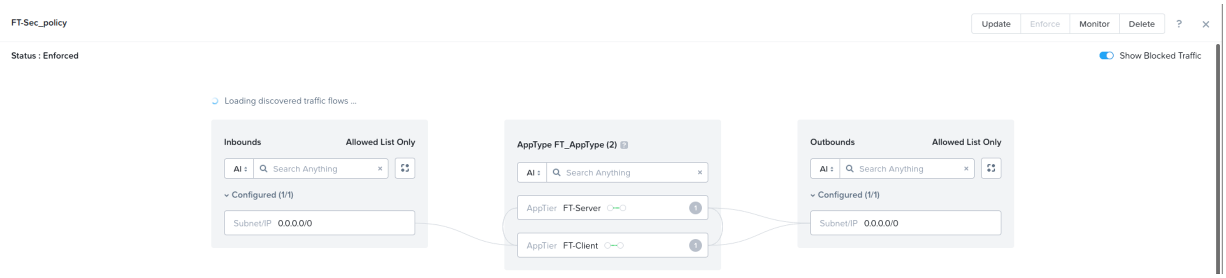
iii. For AppTier: FT-Client, create an outbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.

iv. For AppTier: FT-Server, create an outbound rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.

v. For AppTier: FT-Client, create a tier-to-tier rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.

vi. For AppTier: FT-Server, create a tier-to-tier rule. In the dialog, select *Redirect through a service chain*, and select FORTIGATE_CHAIN. Save.

i. Under *Select a Policy mode*, select *Enforce*. Click *Save and Enforce*.



FT-Sec_policy

Status : Enforced

Loading discovered traffic flows ...

Inbounds — Allowed List Only

Configured (1/1)

Subnet/IP 0.0.0.0/0

AppType FT_AppType (2)

AppTier FT-Server

AppTier FT-Client

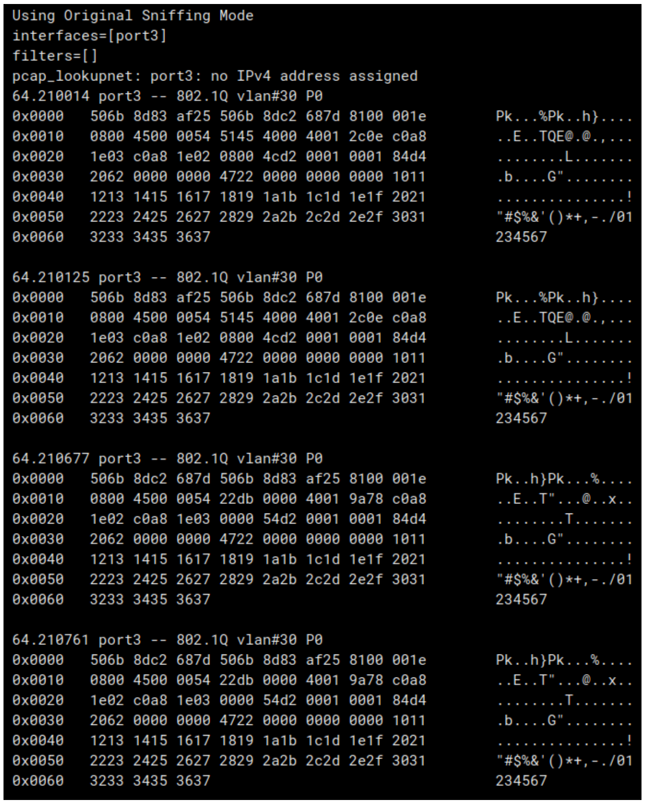
Outbounds — Allowed List Only

Configured (1/1)

Subnet/IP 0.0.0.0/0

To verify that FortiGate-VM unified threat management works:

1. Verify that pings from PC3 to PC2 go through the FortiGate-VM.
2. Run `diagnose sniffer packet port 3 '' 6` to capture ICMP traffic with the vlan30 tag. The following shows example output for this command:



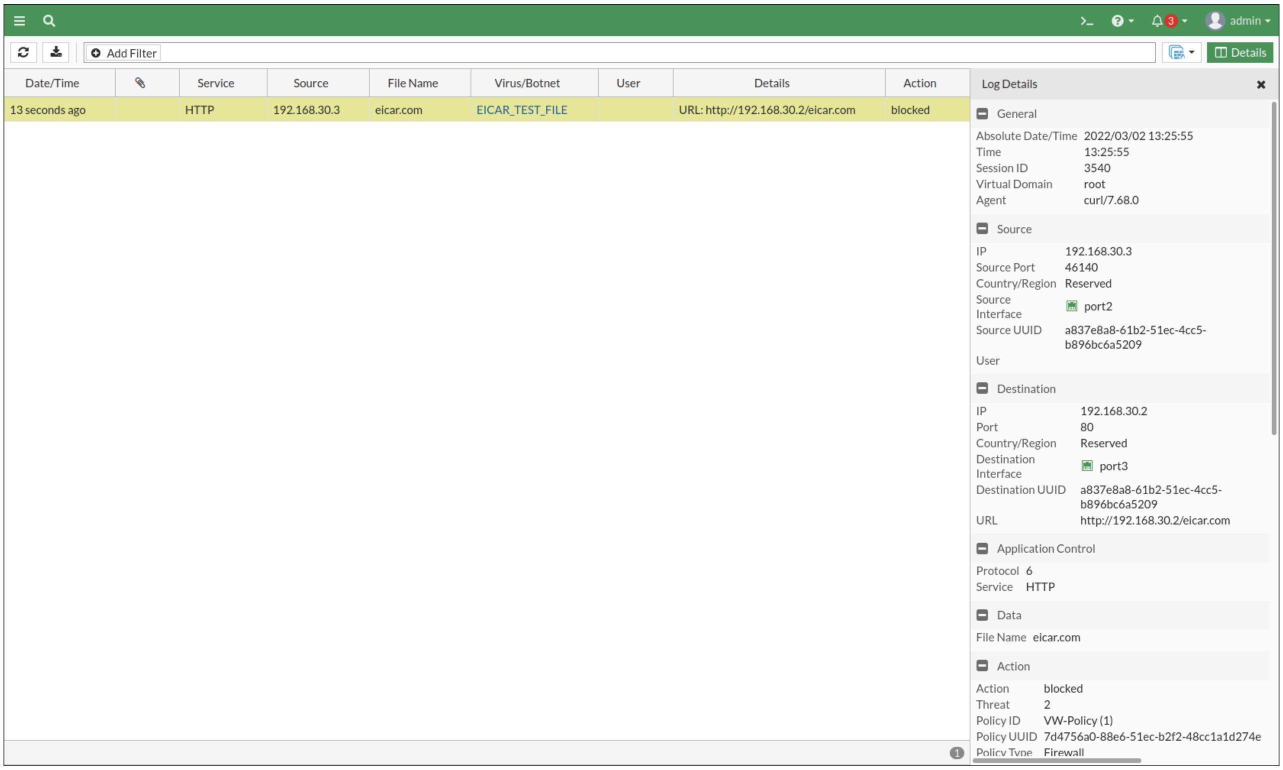
```
Using Original Sniffing Mode
interfaces=[port3]
filters=[]
pcap_lookupnet: port3: no IPv4 address assigned
64.210014 port3 -- 802.1Q vlan#30 P0
0x0000   506b 8d83 af25 506b 8dc2 687d 8100 001e        Pk...%Pk..h}....
0x0010   0800 4500 0054 5145 4000 4001 2c0e c0a8        ..E..TQE@.@.,...
0x0020   1e03 c0a8 1e02 0800 4cd2 0001 0001 84d4        ........L.......
0x0030   2062 0000 0000 4722 0000 0000 0000 1011        .b....G"........
0x0040   1213 1415 1617 1819 1a1b 1c1d 1e1f 2021        ...............!
0x0050   2223 2425 2627 2829 2a2b 2c2d 2e2f 3031        "#$%&'()*+,-./01
0x0060   3233 3435 3637                                 234567

64.210125 port3 -- 802.1Q vlan#30 P0
0x0000   506b 8d83 af25 506b 8dc2 687d 8100 001e        Pk...%Pk..h}....
0x0010   0800 4500 0054 5145 4000 4001 2c0e c0a8        ..E..TQE@.@.,...
0x0020   1e03 c0a8 1e02 0800 4cd2 0001 0001 84d4        ........L.......
0x0030   2062 0000 0000 4722 0000 0000 0000 1011        .b....G"........
0x0040   1213 1415 1617 1819 1a1b 1c1d 1e1f 2021        ...............!
0x0050   2223 2425 2627 2829 2a2b 2c2d 2e2f 3031        "#$%&'()*+,-./01
0x0060   3233 3435 3637                                 234567

64.210677 port3 -- 802.1Q vlan#30 P0
0x0000   506b 8dc2 687d 506b 8d83 af25 8100 001e        Pk..h}Pk...%....
0x0010   0800 4500 0054 22db 0000 4001 9a78 c0a8        ..E..T"...@..x..
0x0020   1e02 c0a8 1e03 0000 54d2 0001 0001 84d4        ........T.......
0x0030   2062 0000 0000 4722 0000 0000 0000 1011        .b....G"........
0x0040   1213 1415 1617 1819 1a1b 1c1d 1e1f 2021        ...............!
0x0050   2223 2425 2627 2829 2a2b 2c2d 2e2f 3031        "#$%&'()*+,-./01
0x0060   3233 3435 3637                                 234567

64.210761 port3 -- 802.1Q vlan#30 P0
0x0000   506b 8dc2 687d 506b 8d83 af25 8100 001e        Pk..h}Pk...%....
0x0010   0800 4500 0054 22db 0000 4001 9a78 c0a8        ..E..T"...@..x..
0x0020   1e02 c0a8 1e03 0000 54d2 0001 0001 84d4        ........T.......
0x0030   2062 0000 0000 4722 0000 0000 0000 1011        .b....G"........
0x0040   1213 1415 1617 1819 1a1b 1c1d 1e1f 2021        ...............!
0x0050   2223 2425 2627 2829 2a2b 2c2d 2e2f 3031        "#$%&'()*+,-./01
0x0060   3233 3435 3637                                 234567
```

3. Go to *Log & Report* > *AntiVirus* and verify that unified threat management blocks an eicar.com sample.



Date/Time	✎	Service	Source	File Name	Virus/Botnet	User	Details	Action
13 seconds ago		HTTP	192.168.30.3	eicar.com	EICAR_TEST_FILE		URL: http://192.168.30.2/eicar.com	blocked

General

Absolute Date/Time	2022/03/02 13:25:55
Time	13:25:55
Session ID	3540
Virtual Domain	root
Agent	curl/7.68.0

Source

IP	192.168.30.3
Source Port	46140
Country/Region	Reserved
Source Interface	port2
Source UUID	a837e8a8-61b2-51ec-4cc5-b896bc6a5209
User	

Destination

IP	192.168.30.2
Port	80
Country/Region	Reserved
Destination Interface	port3
Destination UUID	a837e8a8-61b2-51ec-4cc5-b896bc6a5209
URL	http://192.168.30.2/eicar.com

Application Control

Protocol	6
Service	HTTP

Data

File Name	eicar.com

Action

Action	blocked
Threat	2
Policy ID	VW-Policy (1)
Policy UUID	7d4756a0-88e6-51ec-b2f2-48cc1a1d274e
Policy Type	Firewall

SDN connector integration with Nutanix

See the *FortiOS Administration Guide*.

Change log

Date	Change Description
2022-03-31	Initial release.

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.