

## FORTIGATE FIREWALL SETUP AND IMPLEMENTATION

### Step 1

Download the new deployment for fortigate from <https://support.fortinet.com/Download/VMImages.aspx>

After all the required registrations you will be able to download.

VMWare  
FFW\_VM64-v7.4.1.F-build2463-FORTINET.out (107 MB)  
[Download](#)

New deployment of FortiGate for VMware  
FFW\_VM64-v7.4.1.F-build2463-FORTINET.out.ovf.zip (106.03 MB)  
[Download](#)

Upgrade from previous version of FortiGate for VMware  
FGT\_VM64-v7.4.1.F-build2463-FORTINET.out (107.02 MB)  
[Download](#)

New deployment of FortiGate for VMware  
FGT\_VM64-v7.4.1.F-build2463-FORTINET.out.ovf.zip (106.04 MB)  
[Download](#)

### Step 2

Open VMware workstation and open a new virtual machine.

Select Fortigate-VM64 and agree to all the conditions

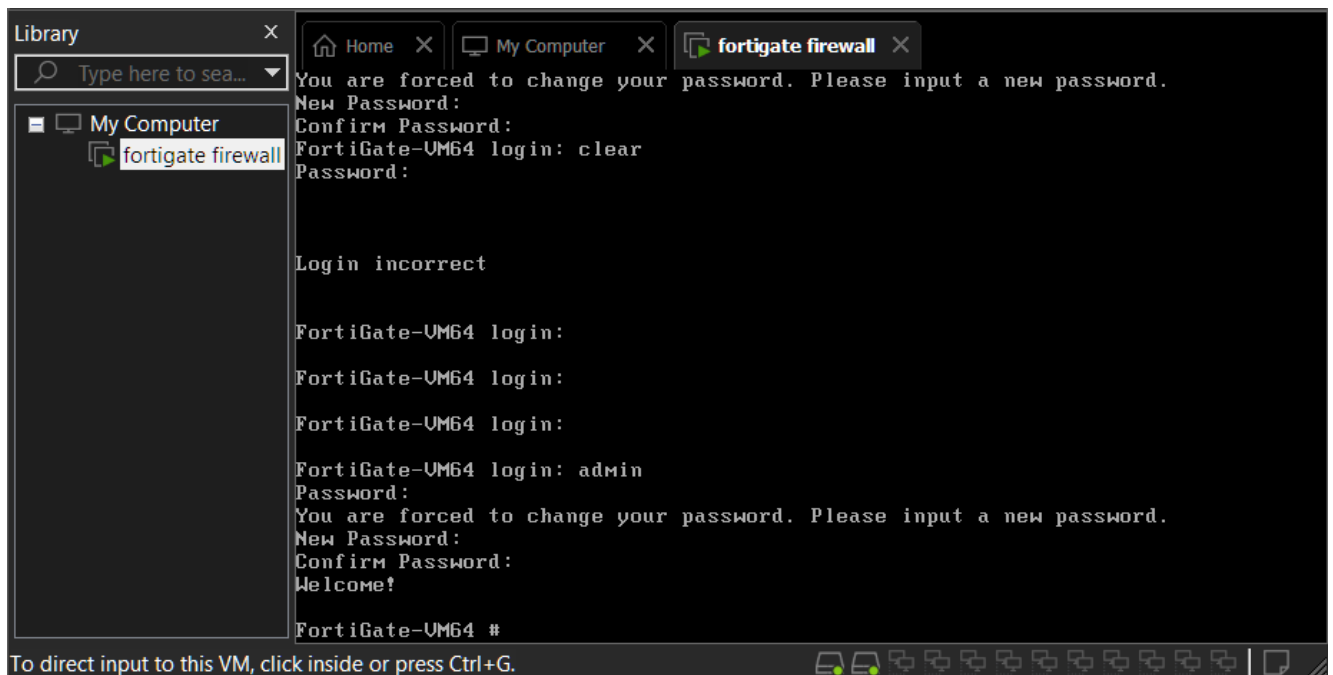
Name	Date modified	Type	Size
Last week			
datadrive.vmdk	30-11-2023 21:27	VMware.VirtualDisk	70 KB
fortios.vmdk	30-11-2023 21:27	VMware.VirtualDisk	1,09,391 KB
readme	30-11-2023 21:27	Text Document	2 KB
FortiGate-VM64.hw13	30-11-2023 21:27	Open Virtualizatio...	30 KB
FortiGate-VM64.hw15	30-11-2023 21:27	Open Virtualizatio...	30 KB
FortiGate-VM64.hw17	30-11-2023 21:27	Open Virtualizatio...	27 KB
FortiGate-VM64.nsxt	30-11-2023 21:27	Open Virtualizatio...	14 KB
FortiGate-VM64	30-11-2023 21:27	Open Virtualizatio...	27 KB
FortiGate-VM64.vapp	30-11-2023 21:27	Open Virtualizatio...	45 KB
FortiGate-VM64-ZTNA.vapp	30-11-2023 21:27	Open Virtualizatio...	29 KB

### Step 3

Customize the bridged adapters as you like and make sure to turn off the connect at power on on all the adapters.

### Step4

You will be probed to create a new password



### Step 5

Type in the following commands

Config system ntp

Set ntpsync disable

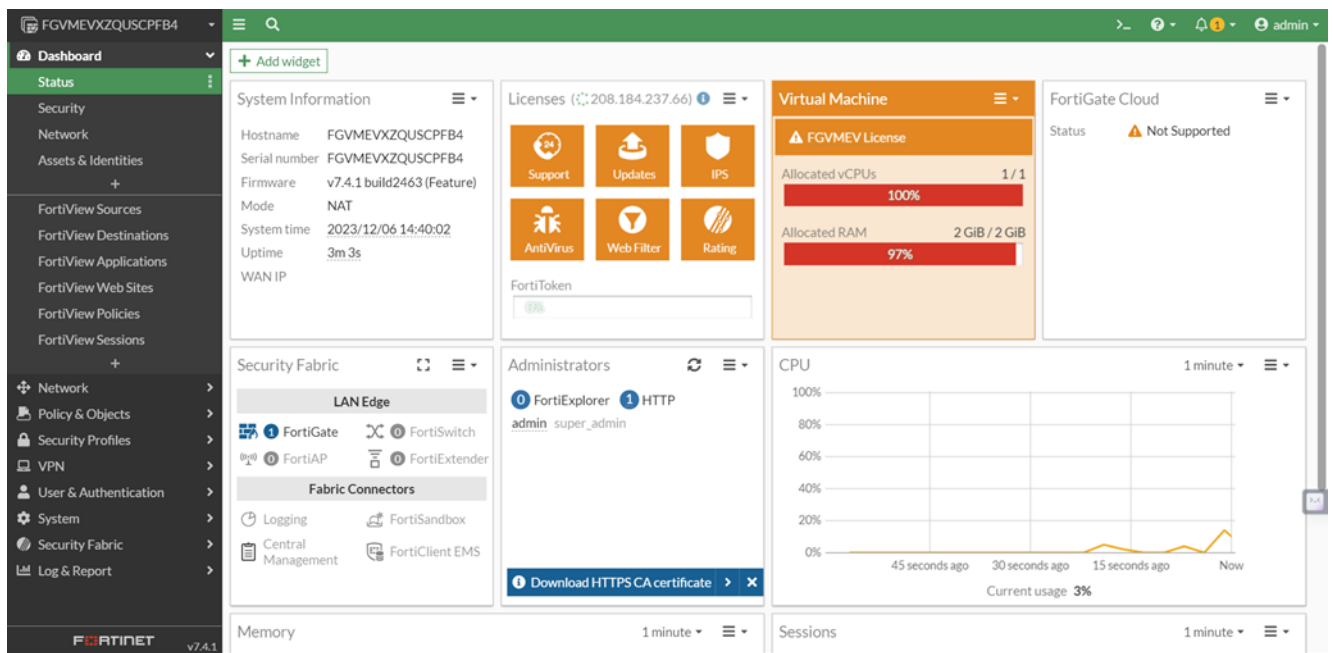
Set type custom

End

### Step 6

Configure port 1 and 2 to allow all the kinds of accessed you might require. Set access mode as dhcp to obtain an ip address manually.

Now using a browser login to that ip address you will get a dashboard like this.



## Step7

Open your wan interface

The screenshot shows the 'Edit Interface' configuration page for the WAN interface (port1). The left sidebar is expanded to show the 'Network' menu, with 'Interfaces' selected. The main content area is divided into two sections:

- Interface Configuration:**
  - Name: WAN (port1)
  - Alias: WAN
  - Type: Physical Interface
  - VRF ID: 0
  - Role: WAN
  - Estimated bandwidth: 0 kbps Upstream, 0 kbps Downstream
  - Dedicated Management Port: ☐
  - Addressing mode: Manual (DHCP)
  - Status: ☒ Connected
  - Obtained IP/Netmask: 192.168.0.4/255.255.255.0 (Renew)
  - Expiry Date: 2023/12/06 16:37:30
  - Acquired DNS: 192.168.0.1
  - Default gateway: 192.168.0.1
  - Retrieve default gateway from server: ☒
  - Distance: 5
  - Override internal DNS: ☒
- Administrative Access:** OK, Cancel buttons.

On the right side, there is a summary section for FortiGate FGVMEVXZQUSCPFB4, showing Active Administrator Sessions (1 HTTP), Status (Up), MAC address (00:0c:29:36:40:86), and Speed Test (Execute speed test button). Additional Information links include API Preview, References, Edit in CLI, Online Guides, Relevant Documentation, Video Tutorials, and Fortinet Community.

## Step 8

For example, we can try setting up a static route. So go into the static route tab

The screenshot shows the 'New Static Route' configuration form in the Fortinet FortiGate web interface. The left sidebar contains the navigation menu with 'Static Routes' selected. The main form area has the following fields:

- Destination:** A dropdown menu with 'Subnet' and 'Internet Service' options. Below it is a text input field containing '0.0.0.0/0.0.0.0'.
- Gateway Address:** A text input field containing '0.0.0.0'.
- Interface:** A dropdown menu with a '+' icon, indicating it is required.
- Administrative Distance:** A text input field containing '10'.
- Comments:** A text input field with the placeholder 'Write a comment...' and a character count '0/255'.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Advanced Options:** A section with a '+' icon and a search bar.

On the right side, there is an 'Additional Information' section with links to 'API Preview', 'Online Guides', 'Relevant Documentation', 'Video Tutorials', 'Fortinet Community', and 'Join the Discussion'. At the bottom of the form are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Static Routes' table in the Fortinet FortiGate web interface. The table has the following columns: Destination, Gateway IP, Interface, Status, and Comments. The table contains one entry:

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	Dynamic Gateway (192.168.0.1)	WAN (port1)	Enabled	

## Step 9

We can try setting up an access control

So go into the firewall policy tab.

Setup a new policy like this

The screenshot shows the 'Edit Policy' window in Fortinet's management interface. The policy is named 'ipv4 policy'. The configuration is as follows:

Field	Value
Name	ipv4 policy
Incoming Interface	internal (port2)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT

**Firewall/Network Options:**

- NAT: ☒ NAT
- IP Pool Configuration: ☒ Use Outgoing Interface Address, ☐ Use Dynamic IP Pool
- Preserve Source Port: ☐ Preserve Source Port
- Protocol Options: ☒ PROT default

**Security Profiles:**

- AntiVirus: ☒ AV default
- Web Filter: ☒ WEB default
- DNS Filter: ☒ DNS default
- Application Control: ☒ APP default

**Additional Information:**

- API Preview
- References
- Edit in CLI
- Online Guides
- Relevant Documentation
- Video Tutorials
- Consolidated Policy Configuration
- Fortinet Community
- Join the Discussion

Buttons: OK, Cancel

ID	Name	Incoming Interface	Outgoing Interface	Schedule	Service	Action	NAT	Standard	Security Profiles	UTM	OB
1	ipv4 policy	internal (port2)	WAN (port1)	always	ALL	ACCEPT	<input checked="" type="checkbox"/>	Standard	AV: default, WEB: default, DNS: default, APP: default	<input checked="" type="checkbox"/>	0 B

## Step 10

Setup an ipv4 dos policy like this

The screenshot shows the 'Create New Policy' window in Fortinet's management interface. The policy is named 'dos\_poli'. The configuration is as follows:

Field	Value
Name	dos_poli
Incoming Interface	internal (port2)
Source Address	all
Destination Address	all
Service	ALL

**L3 Anomalies:**

Name	Logging	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000
ip_dst_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000

**L4 Anomalies:**

Name	Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	2000

**Additional Information:**

- API Preview
- Online Guides
- Relevant Documentation
- Video Tutorials
- Consolidated Policy Configuration
- Fortinet Community
- Join the Discussion

Buttons: OK, Cancel

FGVMEVXZQUSCPFB4

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

Create New

Edit

Edit in CLI

Delete

Search

Export

ID	Name	Interface	Source Address	Destination Address	Service
1	dos_poli	internal (port2)	all	all	ALL

FORTINETv7.4.1

0 Security Rating Issues

Updated: 09:43:36