



# Install Guide

for FortiWeb-VM™ 4.0 MR3 Patch 7

Courtney Schwartz

Contributors:  
George Csaba  
Kazunori Miyanishi  
Idan Soen



# Contents

<b>Overview of FortiWeb-VM .....</b>	<b>4</b>
<b>Architecture .....</b>	<b>4</b>
<b>Licensing .....</b>	<b>5</b>
Evaluation .....	5
<b>Scope .....</b>	<b>6</b>
<b>Conventions .....</b>	<b>6</b>
IP addresses.....	6
Cautions, notes, & tips.....	6
Typographical conventions.....	6
Command syntax conventions.....	7
<b>System requirements .....</b>	<b>10</b>
<b>Downloading the FortiWeb-VM software &amp; registering with Technical Support .....</b>	<b>11</b>
<b>Deploying FortiWeb-VM on VMware vSphere .....</b>	<b>13</b>
Deploying the OVF file.....	14
<b>Configuring the virtual appliance's virtual hardware settings .....</b>	<b>19</b>
Resizing the virtual disk (vDisk).....	19
Configuring the number of virtual CPUs (vCPUs).....	24
Configuring the virtual RAM (vRAM) limit .....	25
Mapping the virtual NICs (vNICs) to physical NICs .....	27
Configuring the vNetwork for the transparent modes.....	29
<b>Powering on the virtual appliance.....</b>	<b>35</b>
<b>Configuring access to the web UI &amp; CLI .....</b>	<b>37</b>
<b>Uploading the license .....</b>	<b>40</b>
Updating the license for more vCPUs.....	44

<b>What's next? .....</b>	<b>47</b>
<b>Updating the virtual hardware .....</b>	<b>47</b>
<b>Index .....</b>	<b>48</b>

# Overview of FortiWeb-VM

Welcome, and thank you for selecting Fortinet products to protect your network.

FortiWeb-VM is a virtual appliance designed specifically to protect web servers.

The FortiWeb family of web application firewalls specializes in layered application threat protection. FortiWeb's integrated web application firewall, DoS prevention, XML firewall and vulnerability scanner protect your web-based applications and Internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting, FortiWeb helps you prevent identity theft, financial fraud and corporate espionage. FortiWeb delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

FortiWeb significantly reduces deployment costs by consolidating a web application firewall, application delivery, XML filtering, web traffic acceleration, and application traffic balancing into a single device. It drastically reduces the time required to protect your internet-facing data and eases the challenges associated with policy enforcement and regulatory compliance.

Its intelligent, application-aware load-balancing engine:

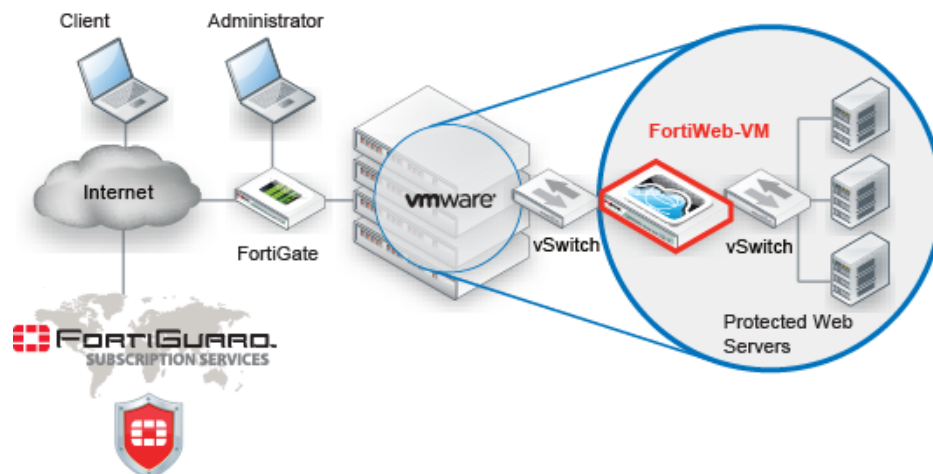
- Increases application performance
- Improves resource utilization
- Improves application stability
- Reduces server response times

## Architecture

FortiWeb-VM is a virtual appliance version of FortiWeb. It is deployed in a virtual machine environment such as VMware vSphere.

Once the virtual appliance is deployed and set up, you can manage FortiWeb-VM via its web UI from a web browser on your management computer.

**Figure 1: FortiWeb-VM architecture**



FortiWeb-VM requires Internet connectivity.

- DNSlookup — UDP 53
- FortiGuard licensing — TCP 443

## Licensing

FortiWeb-VM licenses are available at three sizing levels.

**Table 1: FortiWeb-VM resource limitations**

	<i>License/model</i>		
	<b>VM02</b>	<b>VM04</b>	<b>VM08</b>
<b>Virtual CPUs</b> (vCPUs)	2	4	8

When you place an order for FortiWeb-VM, Fortinet emails a registration number to the recipient address you supplied on the order form. Enter that registration number on the Fortinet Technical Support web site:

<https://support.fortinet.com/>

to register your appliance with Technical Support and to obtain a license file. The license file is required to permanently activate FortiWeb-VM. For details, see “[Downloading the FortiWeb-VM software & registering with Technical Support](#)” on page 11.



**Note:** FortiWeb-VM *requires* an Internet connection to periodically re-validate its license. ***It cannot be evaluated in offline, closed network environments.*** If FortiWeb-VM cannot contact Fortinet’s FDN for 24 hours, access to the web UI and CLI will be locked. The web UI may display a message such as:

```
License has already been uploaded, please wait for authentication  
with registration servers
```

To regain access, restore the Internet connection, then either wait up to 30 minutes for the next license query or reboot the appliance to trigger an immediate license query.

## Evaluation

FortiWeb-VM includes a free 15-day trial license that includes all features except FortiGuard updates. You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiWeb-VM.

Once the trial expires, most functionality is disabled. You will need to purchase a license to continue using FortiWeb-VM.



**Note:** Technical support is *not* included with the 15-day free trial license included with FortiWeb-VM.

# Scope

This document describes how to deploy a FortiWeb virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

This document does **not** cover initial configuration of the virtual appliance itself, nor ongoing use and maintenance. After deploying the virtual appliance, for information on initial appliance configuration, see the *FortiWeb Administration Guide*.

This document is intended for administrators, not end users. If you have a user account on a computer that accesses web sites through a FortiWeb appliance, please contact your system administrator.

# Conventions

Fortinet technical documentation uses the conventions described below.

## IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at:

<http://ietf.org/rfc/rfc1918.txt?number-1918>

For example, even though a real network's Internet-facing IP address would be routable on the public Internet, in this document's examples, it would be shown as a non-Internet-routable IP such as 10.0.0.1, 192.168.0.1, or 172.16.0.1.

## Cautions, notes, & tips

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.



**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.



**Note:** Presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.



**Tip:** Highlights useful additional information, often tailored to your workplace activity.

## Typographical conventions

Fortinet documentation uses the following typographical conventions:

**Table 2: Typographical conventions in Fortinet technical documentation**

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments           : (null) opmode             : nat</pre>
Emphasis	HTTP connections are <b>not</b> secure and can be intercepted by a third party.
File content	<pre>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</pre>
Hyperlink	<a href="https://support.fortinet.com">https://support.fortinet.com</a>
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <i>VPN &gt; IPSEC &gt; automatic Key (IKE)</i> .
Publication	For details, see the <i>FortiGate Administration Guide</i> .

## Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

**Table 3: Command syntax notation**

Convention	Description
<b>Square brackets</b> [ ]	A non-required (optional) word or words. For example: <pre>[verbose {1   2   3}]</pre> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <pre>verbose 3</pre>
<b>Curly braces</b> { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
<b>Options delimited by vertical bars</b>	Mutually exclusive options. For example: <pre>{enable   disable}</pre> indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.

**Table 3: Command syntax notation**

Convention	Description
<p><b>Options delimited by spaces</b></p>	<p>Non-mutually exclusive options. For example:</p> <pre>{http https ping snmp ssh telnet}</pre> <p>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:</p> <pre>ping https ssh</pre> <p><b>Note:</b> To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type:</p> <pre>ping https snmp ssh</pre> <p>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</p>
<p><b>Angle brackets &lt; &gt;</b></p>	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore ( <code>_</code> ) and suffix that indicates the valid data type. For example:</p> <pre>&lt;retries_int&gt;</pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> <li>• <code>&lt;xxx_name&gt;</code> — A name referring to another part of the configuration, such as <code>policy_A</code>.</li> <li>• <code>&lt;xxx_index&gt;</code> — An index number referring to another part of the configuration, such as 0 for the first static route.</li> <li>• <code>&lt;xxx_pattern&gt;</code> — A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all e-mail addresses ending in <code>@example.com</code>.</li> <li>• <code>&lt;xxx_fqdn&gt;</code> — A fully qualified domain name (FQDN), such as <code>mail.example.com</code>.</li> <li>• <code>&lt;xxx_email&gt;</code> — An email address, such as <code>admin@mail.example.com</code>.</li> <li>• <code>&lt;xxx_url&gt;</code> — A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet.com/</code>.</li> <li>• <code>&lt;xxx_ipv4&gt;</code> — An IPv4 address, such as <code>192.168.1.99</code>.</li> </ul>

**Table 3: Command syntax notation**

Convention	Description
	<ul style="list-style-type: none"><li>• <code>&lt;xxx_v4mask&gt;</code> — A dotted decimal IPv4 netmask, such as 255.255.255.0.</li><li>• <code>&lt;xxx_ipv4mask&gt;</code> — A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.</li><li>• <code>&lt;xxx_ipv4/mask&gt;</code> — A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.99/24.</li><li>• <code>&lt;xxx_ipv6&gt;</code> — A colon( : )-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.</li><li>• <code>&lt;xxx_v6mask&gt;</code> — An IPv6 netmask, such as /96.</li><li>• <code>&lt;xxx_ipv6mask&gt;</code> — An IPv6 address and netmask separated by a space.</li><li>• <code>&lt;xxx_str&gt;</code> — A string of characters that is <b>not</b> another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the <a href="#">FortiWeb CLI Reference</a>.</li><li>• <code>&lt;xxx_int&gt;</code> — An integer number that is <b>not</b> another data type, such as 15 for the number of minutes.</li></ul>

# System requirements

Before you can install FortiWeb-VM, you must first have virtual machine (VM) environment software (a hardware abstraction layer (HAL) that is sometimes called a hypervisor) on your server. FortiWeb-VM is a virtual appliance that runs inside that environment.

Supported hypervisor versions include:

- VMware vSphere ESX 4.0/4.1
- VMware vSphere ESXi 4.0/4.1
- VMware vSphere Hypervisor 4.0/4.1/5.0



**Tip:** For best performance, install FortiWeb-VM on a “bare metal” hypervisor, such as VMware ESXi. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host will have fewer computing resources available due to the host OS's own overhead.

For installation instructions, see the documentation for your VM environment, such as:

- <http://www.vmware.com/products/esxi>
- [http://www.vmware.com/support/pubs/vs\\_pages/vsp\\_pubs\\_esxi41\\_e\\_vc41.html](http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esxi41_e_vc41.html)

You must also have the VM environment client, such as VMware vSphere Client, installed on a management computer. (A management computer is a desktop or a laptop that you will use to deploy and manage your virtual machines.)

# Downloading the FortiWeb-VM software & registering with Technical Support

When purchasing FortiWeb-VM from your reseller, you will receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase for technical support.

**Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration.**

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

## To register & download FortiWeb-VM and your license

- 1 On your management computer, start a web browser.
- 2 Log in to the Fortinet Technical Support web site:

<https://support.fortinet.com/>

The screenshot shows the Fortinet Customer Service & Support website. The navigation bar includes 'Home', 'Asset Management', 'Assistance Center', 'Download', 'Support Programs', 'Tools & Resources', 'FortiGuard Center', and 'Feedback'. The main content area is titled 'CUSTOMER SERVICE & SUPPORT' and is divided into several quadrants. The 'Asset Management' quadrant includes links for 'Register/Renew', 'Manage/View Products', and 'Purchase Service'. The 'Assistance Center' quadrant includes 'Create a Ticket', 'Search/View Tickets', and 'Web Chat'. The 'Download' quadrant includes 'FortiGuard Service Updates', 'Firmware Images', and 'Firmware Image Checksums'. The 'Feedback' quadrant includes 'Knowledge Base Survey' and 'Feedback'. The 'Support Programs' quadrant includes 'Support Offerings', 'Premium Support', 'Premium RMA', and 'Professional Services'. The 'Tools & Resources' quadrant includes 'Knowledge Base', 'Technical Documentation', 'Discussion Forums', 'Training & Certification', and 'FortiGuard Blog'. The 'FortiGuard Center' quadrant includes 'Advisories & Reports', 'FortiGuard Services', 'Security Tools', 'Resource Library', and 'Global Threat Levels'. On the right side, there is a sidebar with 'IMPORTANT INFO' and a 'RESOURCE CENTER' containing links for 'Registration Guide', 'Ticket Creation Guide', 'Online RMA Form', 'CSS Reference Guide', 'Forti-Companion', and 'Product Life Cycle'.

- 3 In the *Asset Management* quadrant of the page, click *Register/Renew*.
- 4 Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated mixture of 25 numbers and characters in groups of 5, such as:

12C45-AB3DE-678G0-F9HIJ-123B5

A registration form will appear.

- 5 Use the form to register your ownership of FortiWeb-VM with Technical Support. After completing the form, a registration acknowledgement page will appear.

- 6 Click the *License File Download* link.  
Your browser will download the `.lic` file that was purchased for that registration number.
- 7 In the upper left corner of the page, click the *Home* link to return to the initial page.
- 8 In the *Download* quadrant of the page, click *Firmware Images*.
- 9 Click the FortiWeb link and navigate to the version that you want to download.
- 10 Download the `.zip` file. You will use this for **new virtual appliance (VM)** installations. Contains a deployable virtual machine package. (`.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)



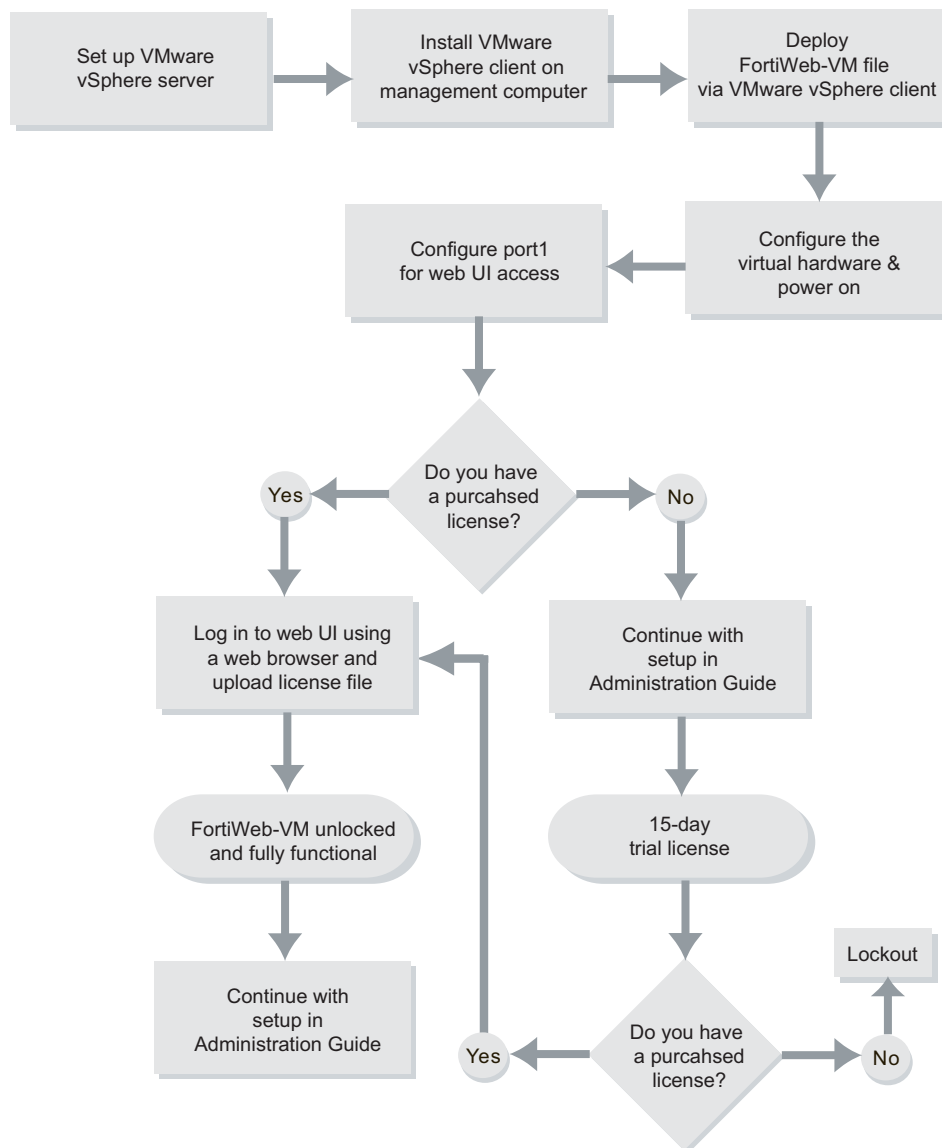
**Note:** Files for FortiWeb-VM have a `FWB_VM` file name prefix. Other prefixes indicate that the file is for hardware versions of FortiWeb such as FortiWeb-3000C. Such other files cannot be used with FortiWeb-VM.

- 11 Extract the `.zip` compressed archive's contents to a folder.
- 12 Continue by deploying the virtual appliance package (see [“Deploying FortiWeb-VM on VMware vSphere” on page 13](#)).

# Deploying FortiWeb-VM on VMware vSphere

The diagram below overviews the process for installing FortiWeb-VM on VMware vSphere, which is described in the subsequent text.

**Figure 2: Basic steps for installing FortiWeb-VM (VMware)**



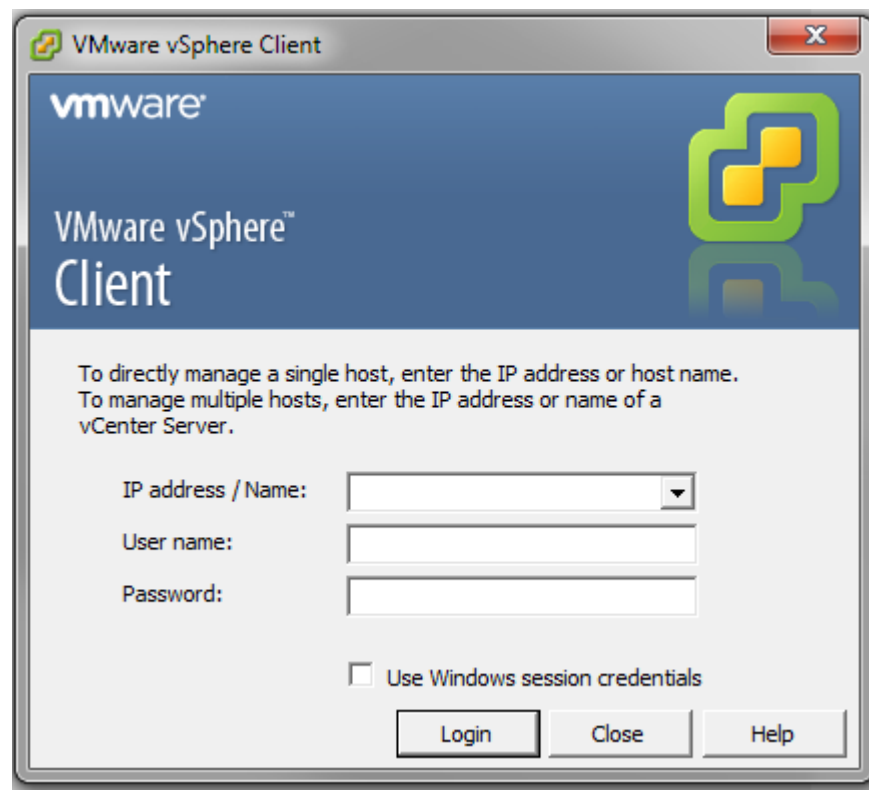
## Deploying the OVF file

Before you can configure FortiWeb-VM, you must first use VMware vSphere Client to deploy the FortiWeb-VM OVF package.

### To deploy the virtual appliance

- 1 On your management computer, start VMware vSphere Client.

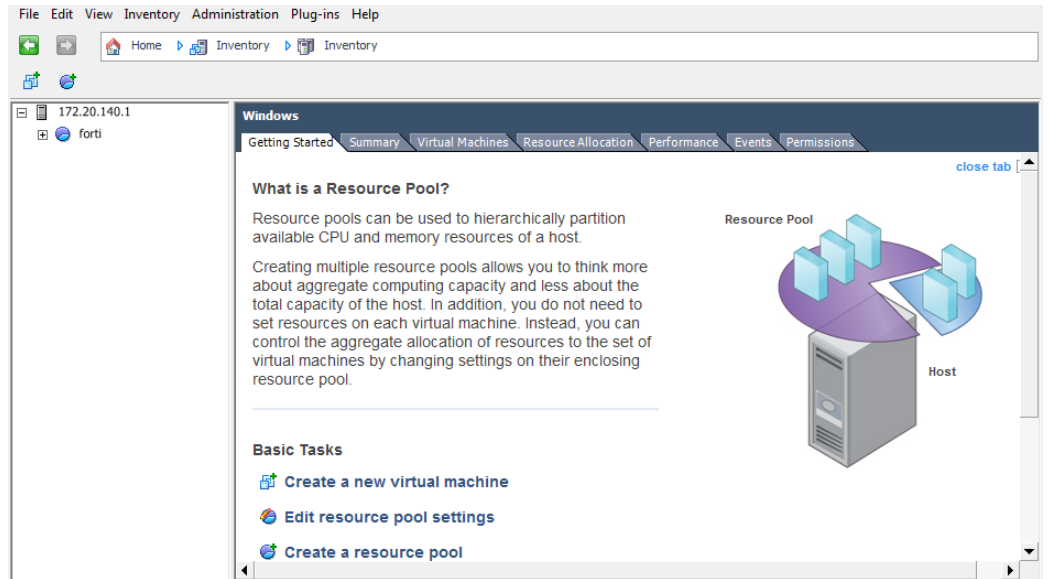
**Figure 3: Starting VMware vSphere Client**



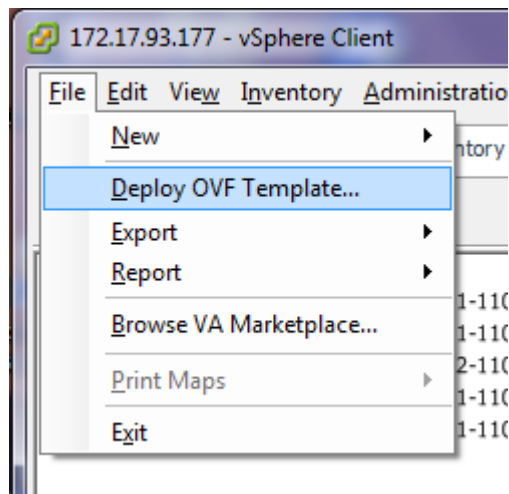
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.

5 Click *Login*.

When you successfully log in, the vSphere Client window appears.

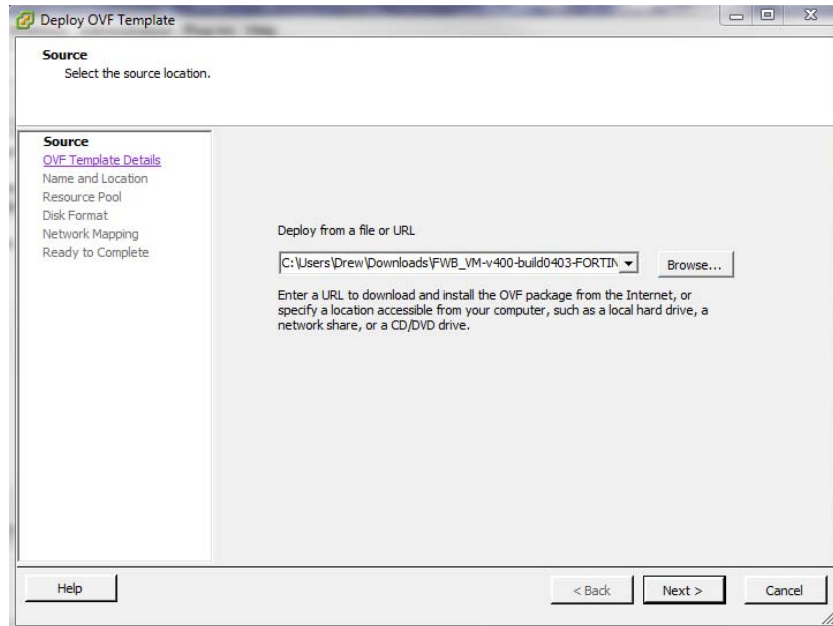


6 Go to *File > Deploy OVF Template*.

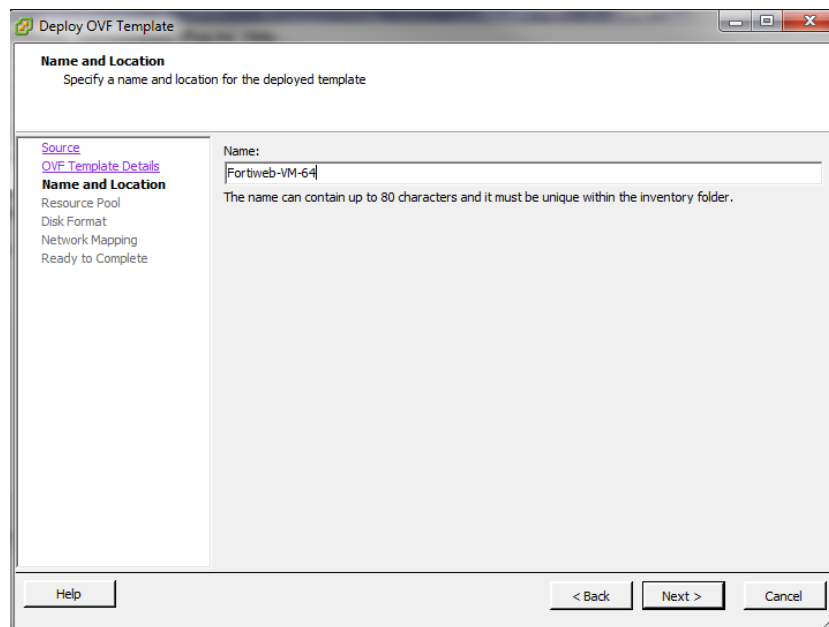


A deployment wizard window appears.

- 7 In the *Deploy OVF Template* window, click *Browse*, then locate the FortiWeb-VM OVF file.

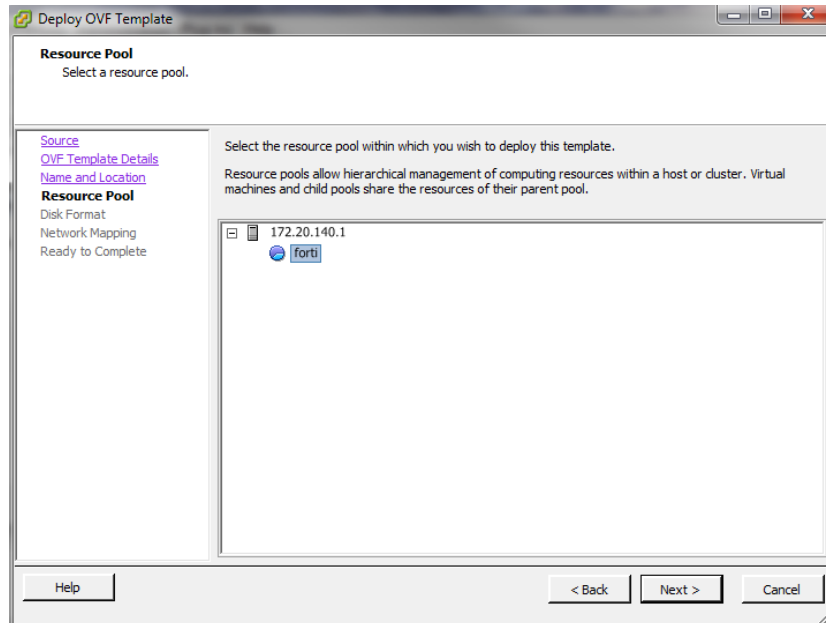


- 8 Click *Next* twice.
- 9 In *Name*, type a unique descriptive name for this instance of FortiWeb-VM as it will appear in vSphere Client's inventory, such as `FortiWeb-VM-64-101`. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiWeb-VM web UI.)



- 10 Click *Next*.

11 In the resource pool tree, select a virtual machine.



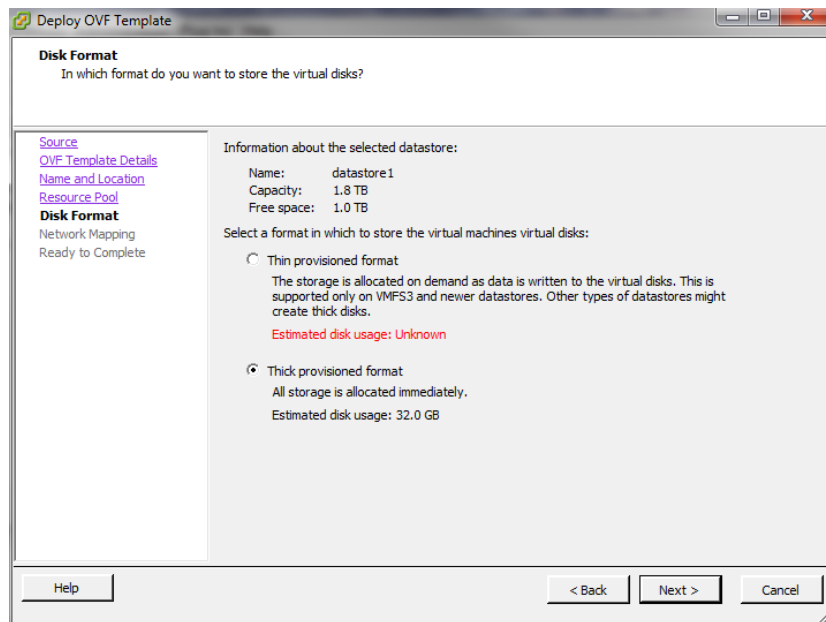
12 Click *Next*.

13 For the storage repository, select either:

- *Thin provisioned format* — Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.
- *Thick provisioned format* — Immediately allocate of disk space (specifically 32 GB) for the storage repository

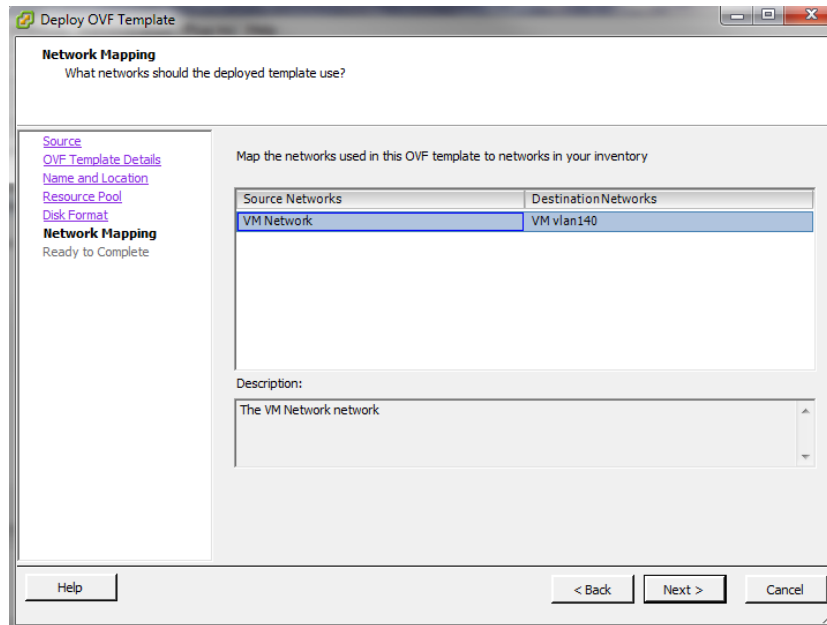


**Note:** Regardless of your choice here, you must later either allocate or make available at least 40 GB of disk space. 32 GB is only the default minimum value, and is not recommended.



14 Click *Next*.

15 If the hypervisor has more than one possible network mapping for its vSwitch, click to select the row for the network mapping that FortiWeb-VM should use.

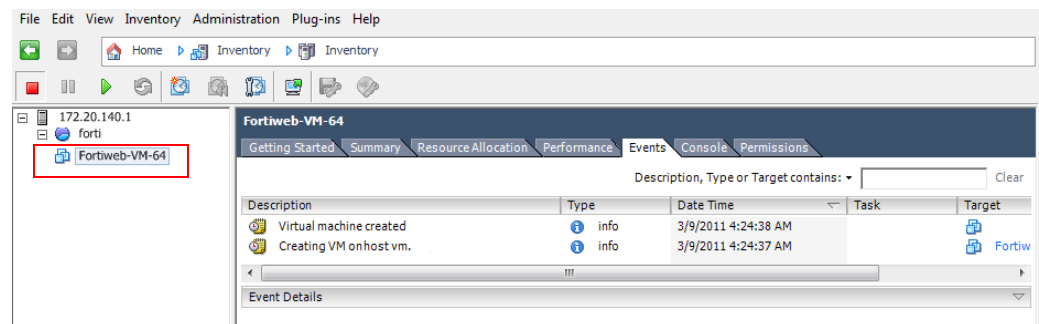


16 Click *Next*.

17 Click *Finish*.

The wizard closes. The client connects to the VM environment and deploys the OVF to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take several minutes to complete.

The vSphere Client window reappears. The navigation pane's list of virtual machines on the left now should include your new instance of FortiWeb-VM.



Continue with "Configuring the virtual appliance's virtual hardware settings" on page 19.



**Note:** Do **not** power on the virtual appliance **until** you:

- Resize the virtual disk (VMDK) (see “Resizing the virtual disk (vDisk)” on page 19)
- Set the number of vCPUs (see “Configuring the number of virtual CPUs (vCPUs)” on page 24)
- Set the vRAM on the virtual appliance (“Configuring the virtual RAM (vRAM) limit” on page 25)
- Map the virtual network adapter(s) (“Mapping the virtual NICs (vNICs) to physical NICs” on page 27).

These settings cannot be configured inside FortiWeb-VM, and must be configured in the VM environment. **Some settings cannot be reconfigured after you power on the virtual appliance.**

## Configuring the virtual appliance’s virtual hardware settings

After installing FortiWeb-VM, log in to VMware vSphere on the server and configure the virtual appliance’s hardware settings to suit the size of your deployment.

For information on the limits of configurable values for FortiWeb-VM, see the [FortiWeb Administration Guide](#).

### Resizing the virtual disk (vDisk)

If you configure the virtual appliance’s storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk **before** powering on.



**Note:** This step is not applicable if the virtual appliance will use external network file system (such as NFS) datastores.

The FortiWeb-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. **Resize the vDisk before powering on the virtual machine.**

Before doing so, make sure that you understand the effects of your vDisk settings.

For example, if you have an 800 GB datastore which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB on your FortiWeb-VM.

Consider also that, depending on the size of your organization’s network, you might require more or less storage for your auto-learning data, anti-defacement backups, scan results, and reports.

For more information on vDisk sizing, see:

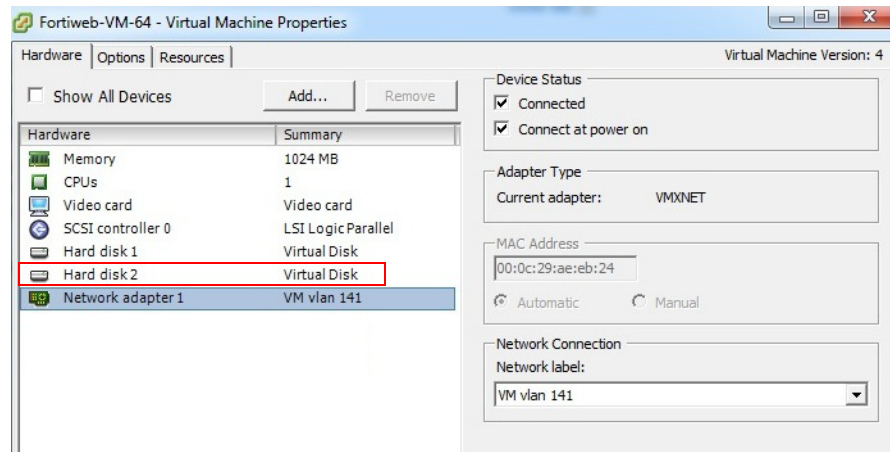
<http://communities.vmware.com/docs/DOC-11920>

#### To resize the vDisk

- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.

- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiWeb-VM-64-101*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.



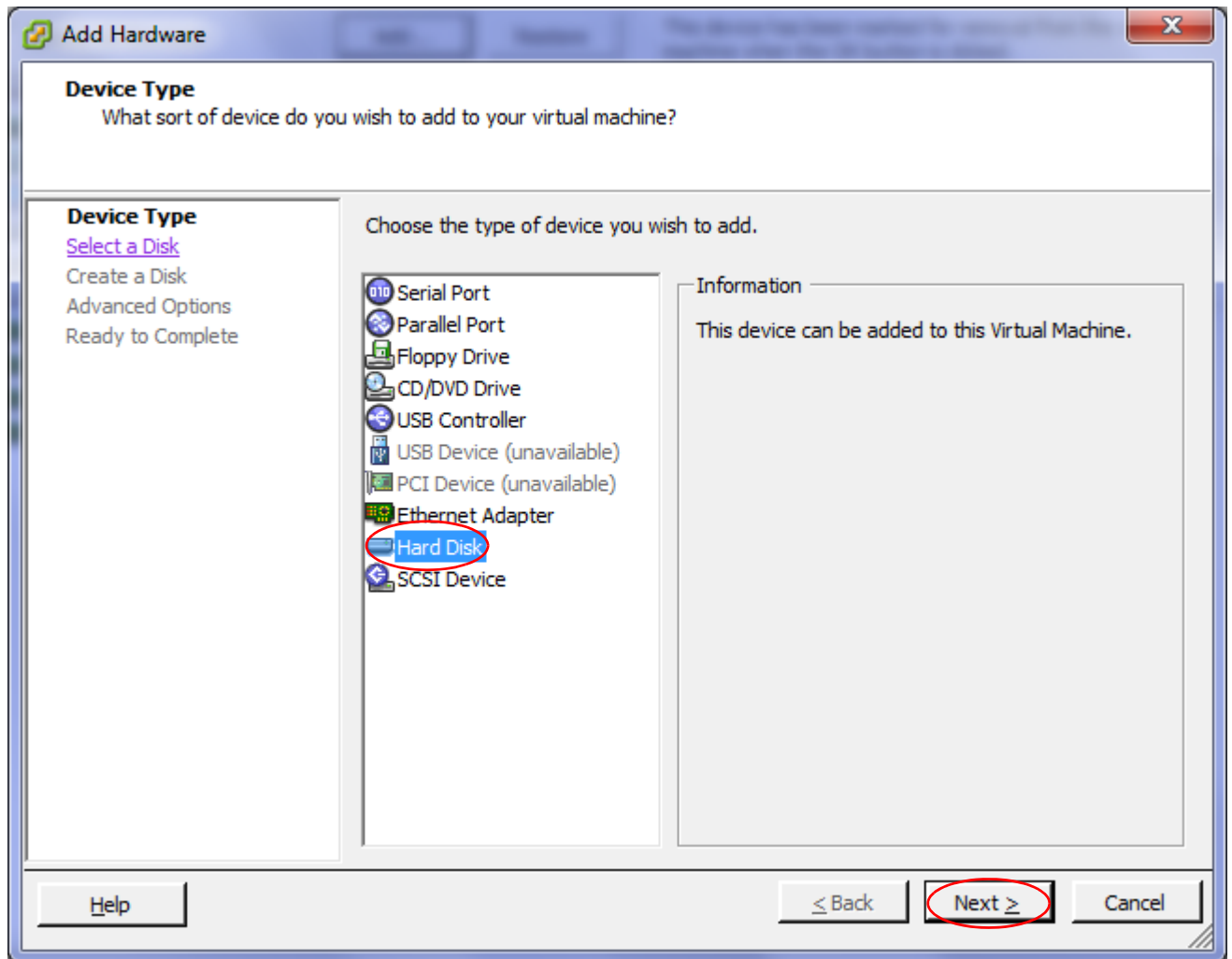
- 7 In the list of virtual hardware on the left side of the dialog, click *Hard disk 2*.

- 8 Click *Remove*.

- 9 Click *Add*.

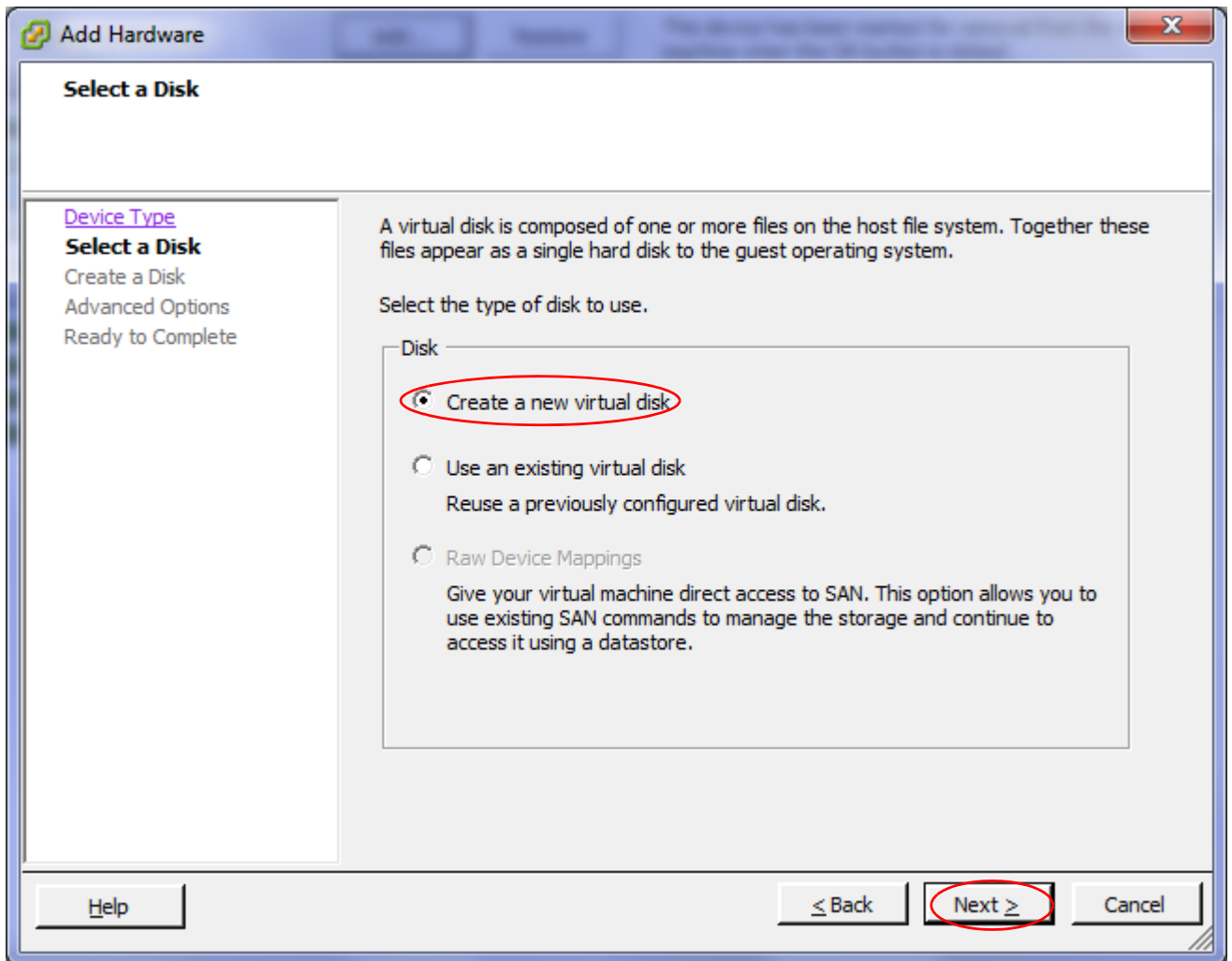
The *Add Hardware* dialog appears.

10 In the list of device types, click *Hard Disk*.



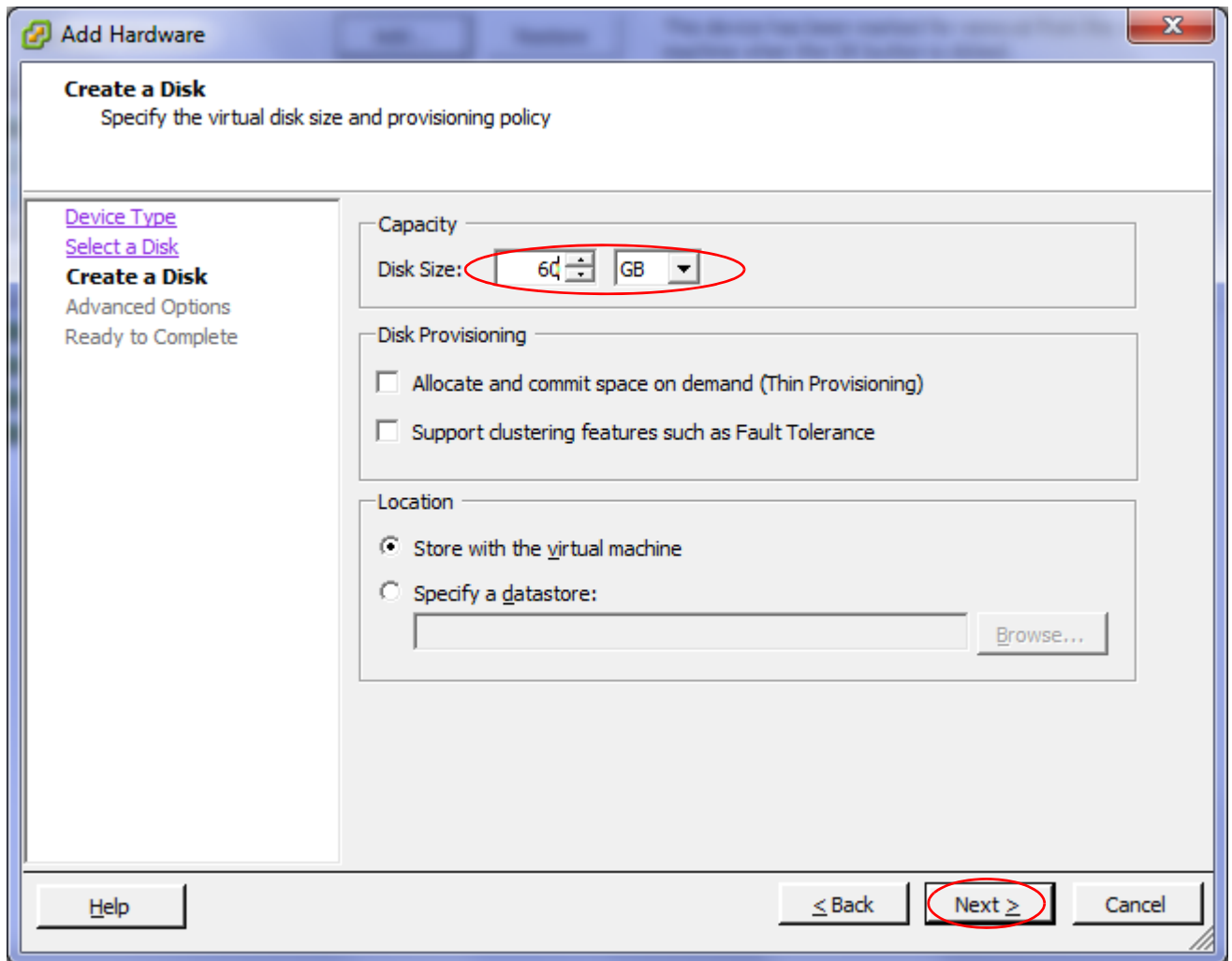
11 Click Next.

12 Select *Create a new virtual disk*.



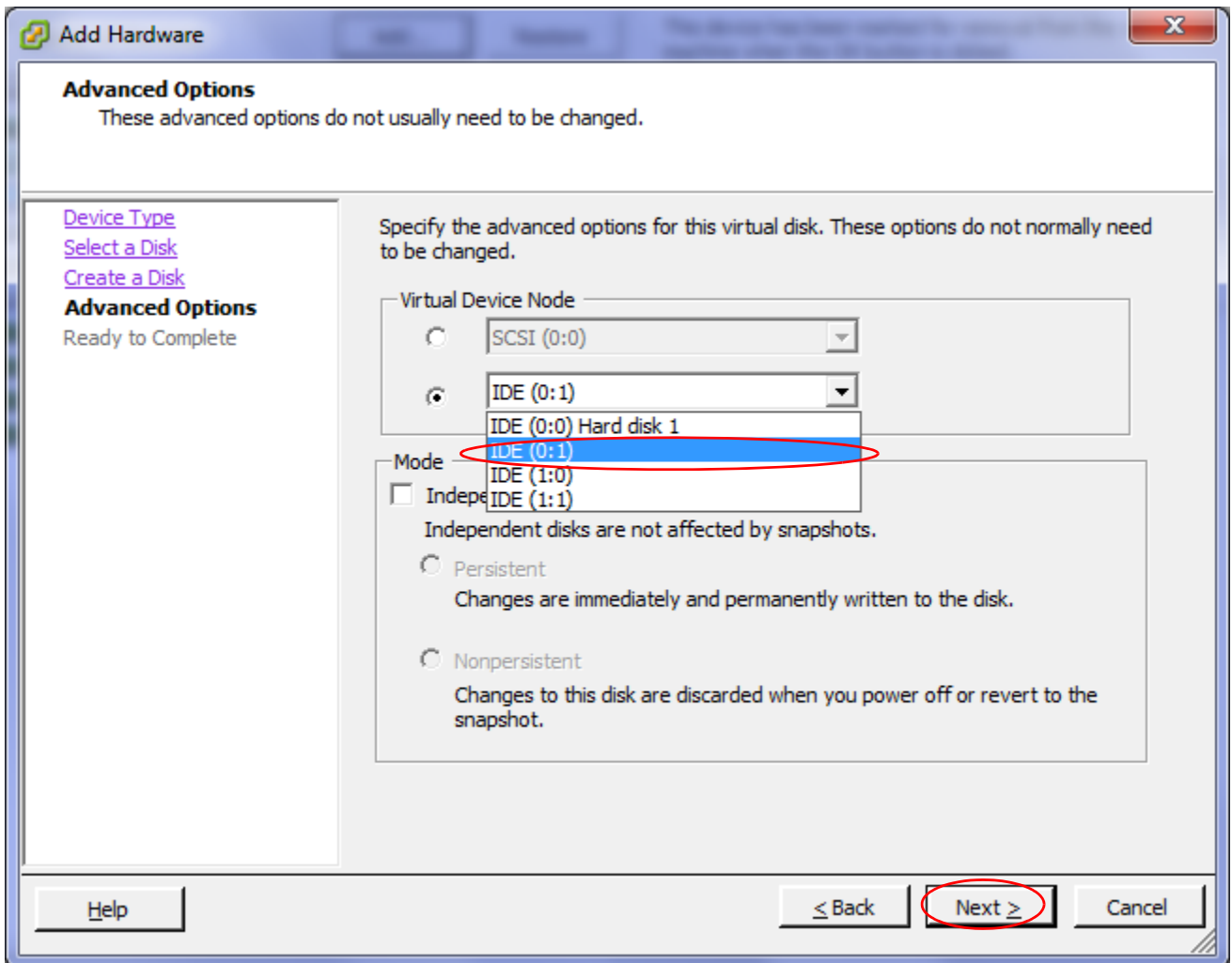
13 Click *Next*.

14 In *Disk Size*, type the new size, in gigabytes (GB), of the vDisk.



15 Click *Next*.

- 16 Select the bottom option in *Virtual Device Node*, then from its drop-down menu, select *IDE (0:1)*.



- 17 Click *Next*.
- 18 Click *Finish*.
- 19 Click *OK*.
- 20 If you do not need to change the other resources, continue with “Powering on the virtual appliance” on page 35. Otherwise continue with “Configuring the number of virtual CPUs (vCPUs)” on page 24.

### Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 2 vCPUs. Depending on the FortiWeb-VM license that you purchased, you can allocate up to 2, 4, or 8 vCPUs.



**Note:** If you need to increase or decrease the vCPUs after the initial boot, power off FortiWeb-VM, adjust the number of vCPUs, then see “Updating the license for more vCPUs” on page 44.

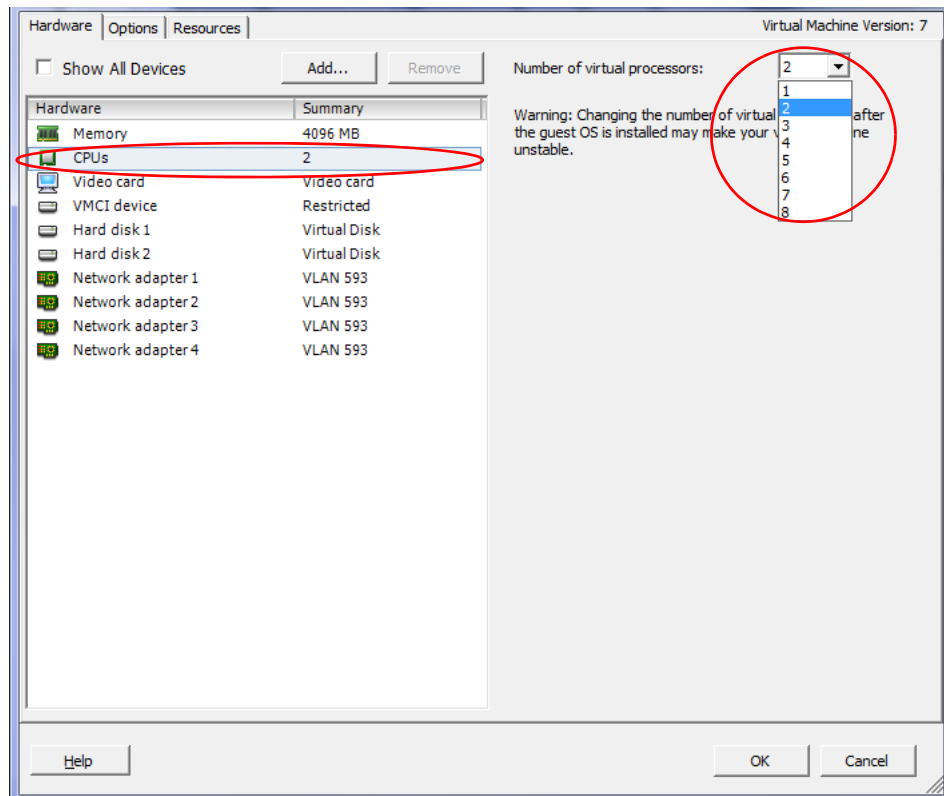
For more information on vCPUs, see the VMware vSphere documentation:

### To change the number of vCPUs

- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiWeb-VM-64-101*, then select *Edit Settings*.

The virtual appliance's properties dialog appears.

- 7 In the list of virtual hardware on the left side of the dialog, click *CPUs*.
- 8 In *Number of virtual processors*, type the maximum number of vCPUs to allocate. Valid values range from 1 to 8.



- 9 Click *OK*.
- 10 If you do not need to change the other resources, continue with “Powering on the virtual appliance” on page 35. Otherwise continue with “Configuring the virtual RAM (vRAM) limit” on page 25.

### Configuring the virtual RAM (vRAM) limit

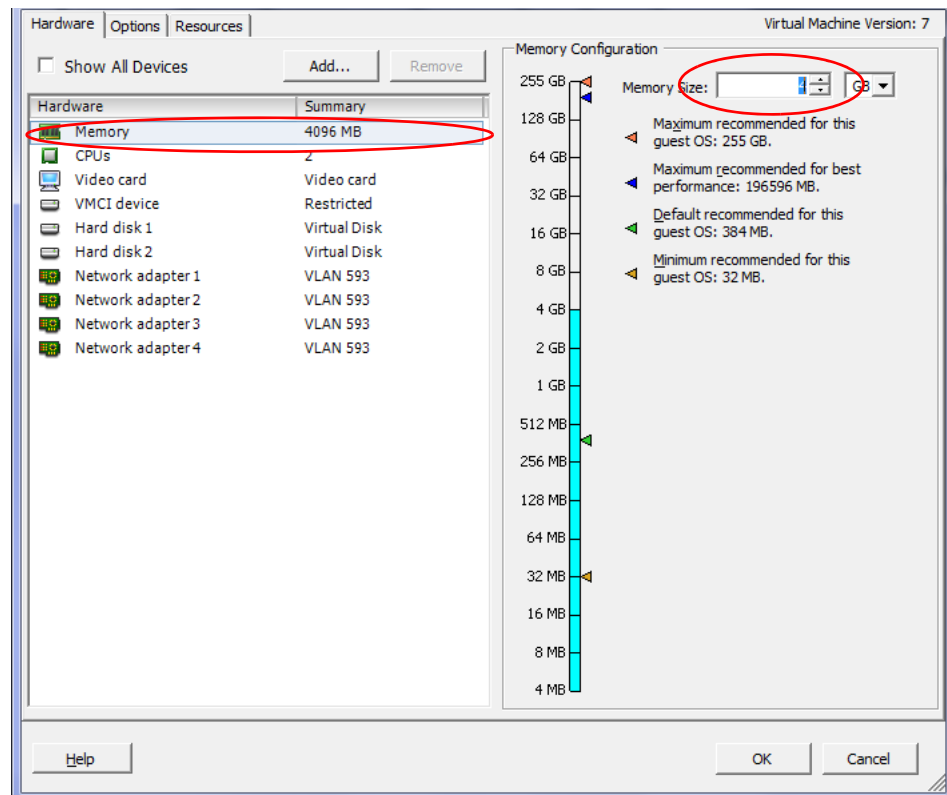
FortiWeb-VM comes pre-configured to use 4 GB of vRAM. You can change this value. The valid range is from 4 GB to 16 GB.



**Note:** It is possible to configure FortiWeb-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

### To change the amount of vRAM

- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, right-click the name of the virtual appliance, such as *FortiWeb-VM-64-101*, then select *Edit Settings*.  
The virtual appliance's properties dialog appears.
- 7 In the list of virtual hardware on the left side of the dialog, click *Memory*.
- 8 In *Memory Size*, type the maximum number in gigabytes (GB) of the vRAM to allocate. Valid values range from 2 to 4.



- 9 Click *OK*.
- 10 If you do not need to change the other resources, continue with “Powering on the virtual appliance” on page 35. Otherwise continue with “Mapping the virtual NICs (vNICs) to physical NICs” on page 27.

## Mapping the virtual NICs (vNICs) to physical NICs

Appropriate mappings of the FortiWeb-VM ports to physical ports depends on your existing virtual environment.



**Tip:** Often, the default bridging vNICs work, and don't need to be changed.

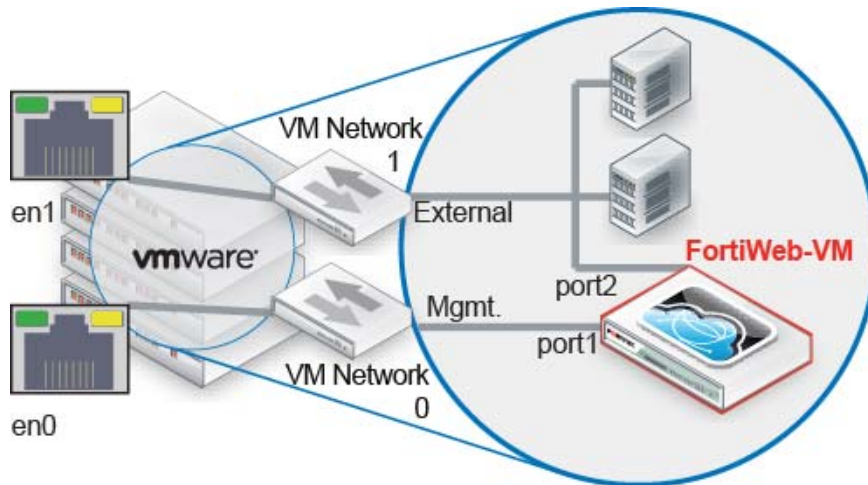
If you are unsure of your network mappings, try bridging first **before** non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines should have their own IP addresses on your network.

The most common exceptions to this rule are for VLANs and the transparent modes. See ["Configuring the vNetwork for the transparent modes"](#) on page 29.

When you deploy the FortiWeb-VM package, 4 bridging vNICs are created and automatically mapped to a port group on 1 virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 4 network interfaces in FortiWeb-VM. (Alternatively, if you prefer, some or all of the network interfaces may be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if either your VM environment requires it or the FortiWeb-VM will be operating in either true transparent proxy or transparent inspection mode. (For information on how to choose the operation mode, see the setup instructions in the [FortiWeb Administration Guide](#).)

[Table 4](#) provides an example of how vNICs could be mapped to the physical network ports on a server.



**Table 4: Example: Network mapping for reverse proxy mode**

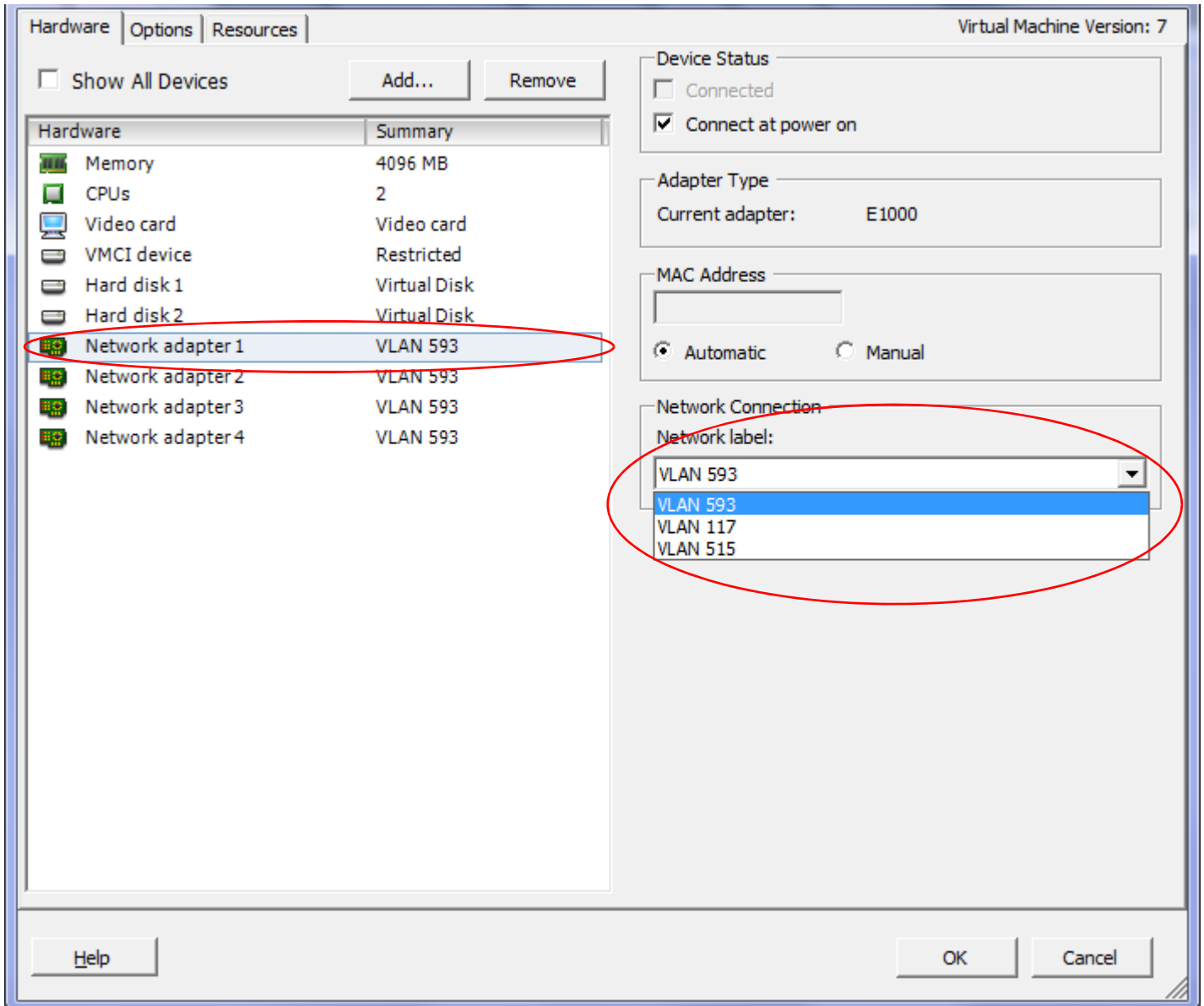
VMware vSphere			FortiWeb-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiWeb-VM	Network Interface Name in Web UI/CLI
eth0	VM Network 0	Management	port1
eth1	VM Network 1	External	port2
eth1	VM Network 2	Internal	port3
eth1	VM Network 1	External	port4

### **To map network adapters**

- 1** On your management computer, start VMware vSphere Client.
- 2** Enter the IP address, user name, and password of the VMware vSphere server.
- 3** Click *Login*.
- 4** In the left pane, right-click the name of the virtual appliance, such as *FortiWeb-VM-64-101*, then select *Edit Settings*.  
The virtual appliance's properties dialog appears.
- 5** In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.

- From the *Network Connection* drop-down menu, select the virtual network mapping for the virtual network adapter.

The correct mapping varies by your virtual environment's network configuration. In the example illustration below, the vNIC *Network adapter 1* is mapped to the virtual network (vNetwork) named *VLAN 593*.



- Click **OK**.
- Continue with "Powering on the virtual appliance" on page 35.

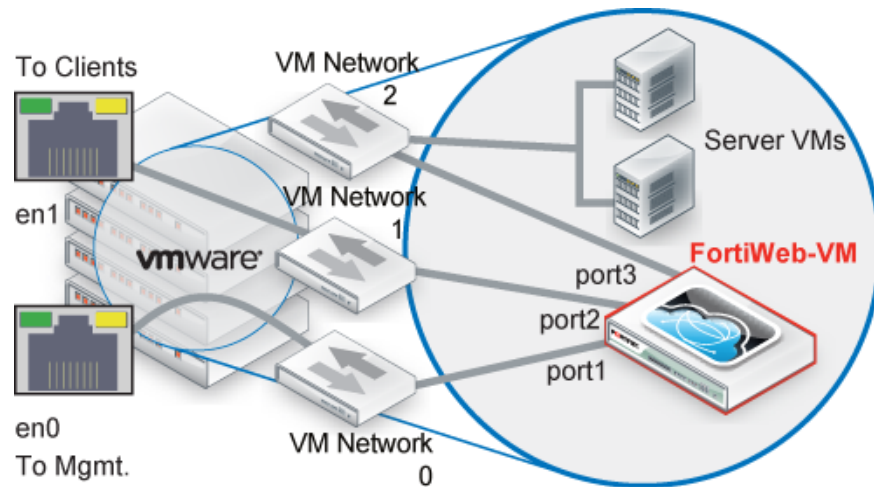
### Configuring the vNetwork for the transparent modes

The default vNetwork configuration does **not** function with FortiWeb bridges (V-zones), which will be used if you deploy your FortiWeb-VM in either true transparent proxy or transparent inspection operation mode.

To support the transparent modes, you **must**:

- add 2 vSwitches or distributed vSwitches (dvSwitch) for the bridge: one for the server side, and one for the client side
- set both to promiscuous mode
- map the new vSwitches to a network adapter

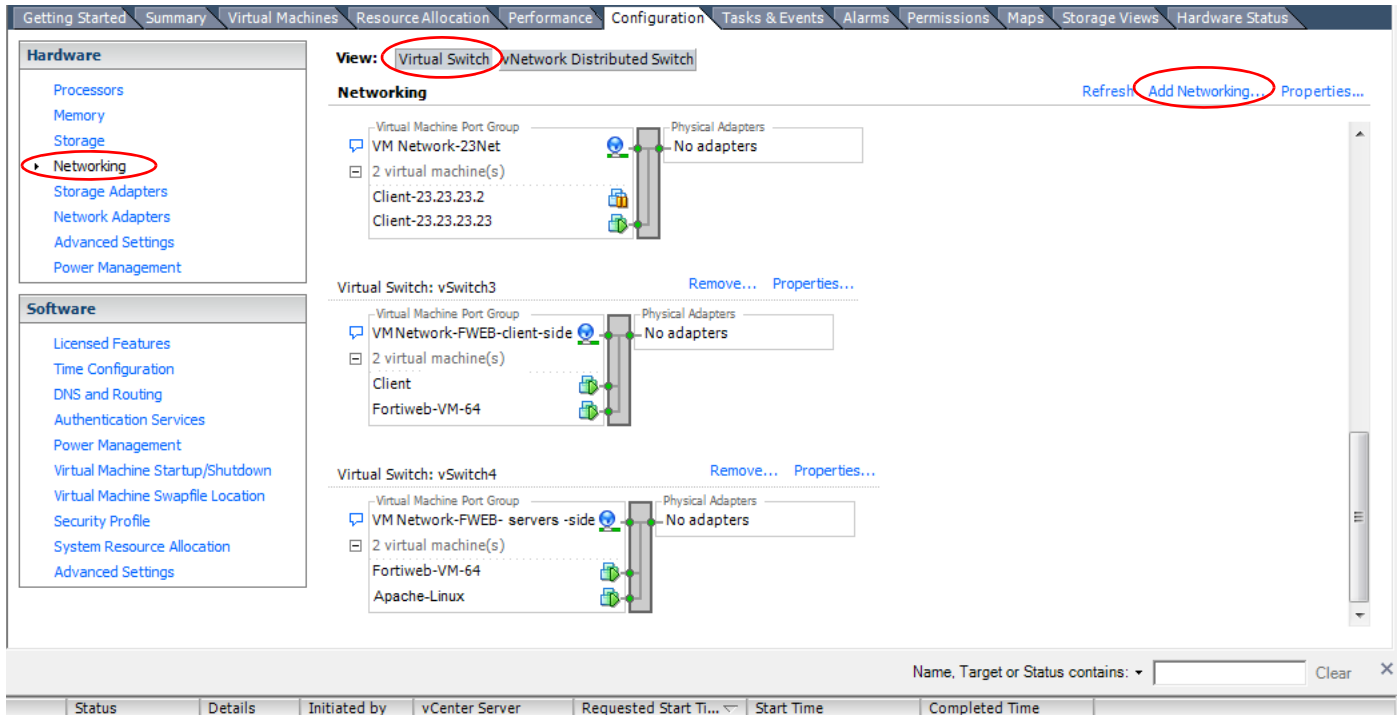
Similar to a deployment that does not use virtual machines, connections between clients and servers will be piped through the two vSwitches that comprise the bridge, with FortiWeb-VM in between them.



#### To create a vSwitch

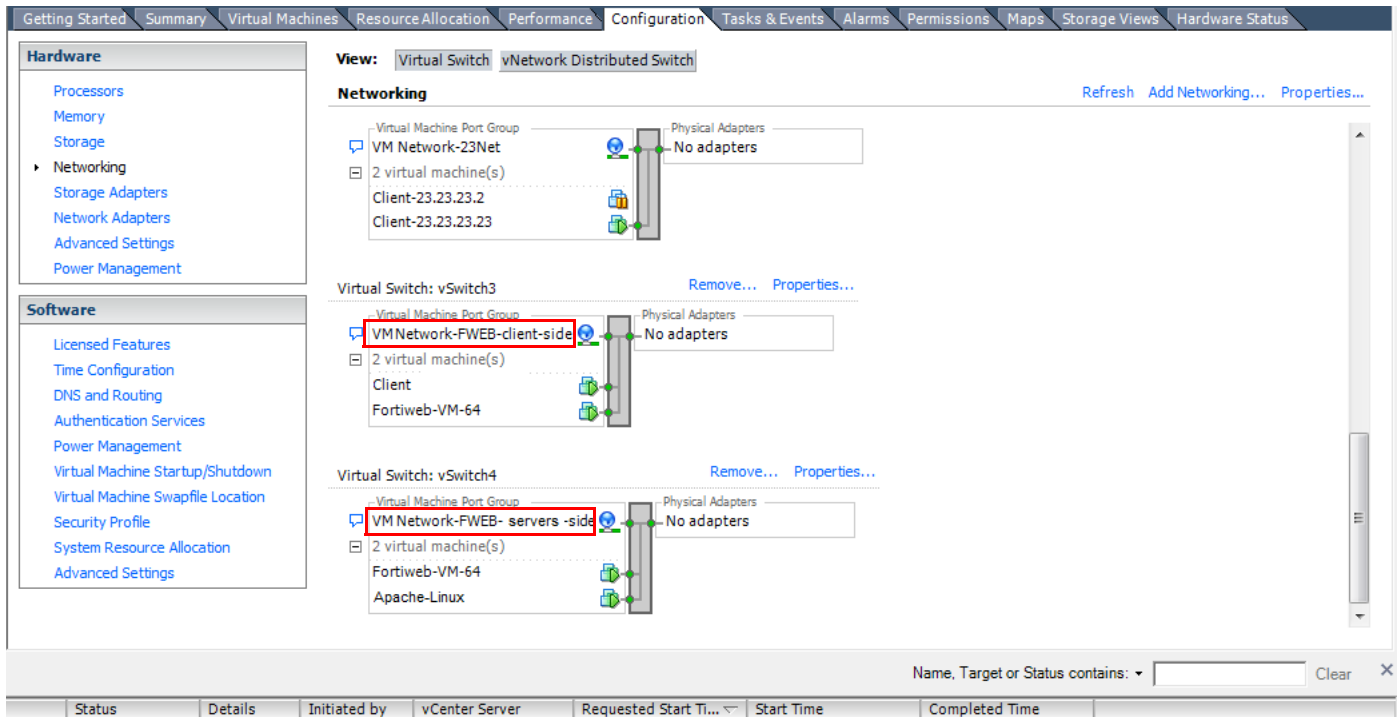
- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, click the name of the virtual appliance, such as *FortiWeb-VM-64-101*.

- On the *Configuration* tab, click *Networking*.  
A window appears where you can configure vSwitches or distributed vSwitches.



- In the *View* set of buttons, click *Virtual Switch*. (If you are configuring a distributed vSwitch, click *vNetwork Distributed Switch* instead. Your steps will vary slightly, but will be similar.)
- Click *Add Networking*.
- Accept the default connection type, *Virtual Machines*, and click *Next*.
- Select *Create a virtual switch*.
- Click *Next*.
- Under *Port Group Properties*, enter a network label such as `Client-Side-vSwitch1` that identifies the port group.
- In *VLAN ID*, if your network uses VLANs, enter a number between 1 and 4,094 to specify the VLAN tag that the vSwitch will use.
- Click *Next*.
- Click *Finish*.

17 Repeat this procedure to create the other vSwitch.

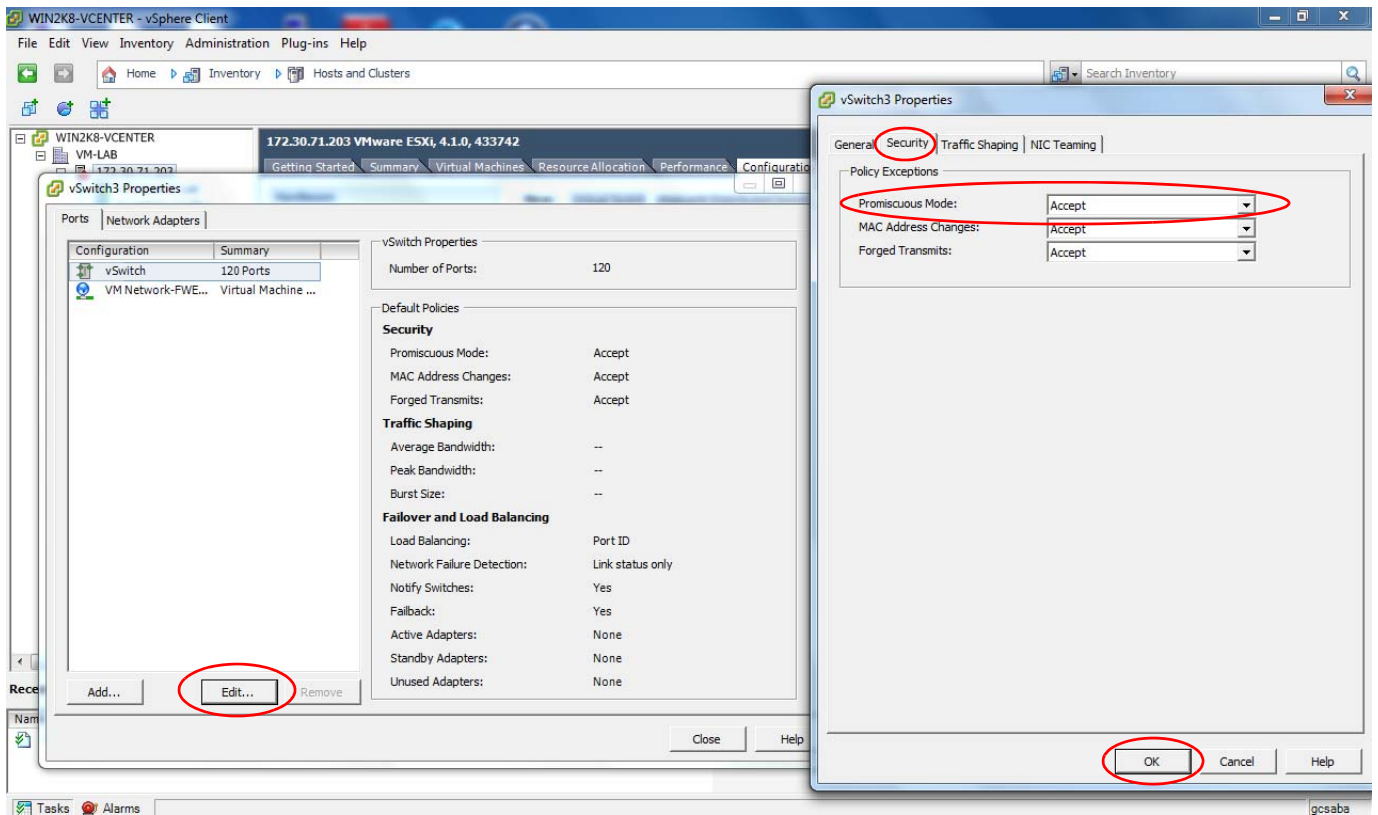


18 Continue with “To configure promiscuous mode for the new vSwitch”.

### To configure promiscuous mode for the new vSwitch

1 On the *Configuration* tab, click *Networking*.

## 2 Select *Properties*.



- 3 Click *Edit*.
- 4 Select the *Security* tab.
- 5 From the drop-down list for *Promiscuous Mode*, select *Accept*.
- 6 Repeat this procedure with the other vSwitch for the bridge.
- 7 Continue with "To map a network adapter to the new vSwitch".

### To map a network adapter to the new vSwitch

- 1 In the left pane, click the name of the virtual appliance, such as *FortiWeb-VM-64-101*.

- 2 On the *Getting Started* tab, select *Edit Virtual Machine Settings*.

**Getting Started** Summary Resource Allocation Performance Events Console Permissions close tab

### What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

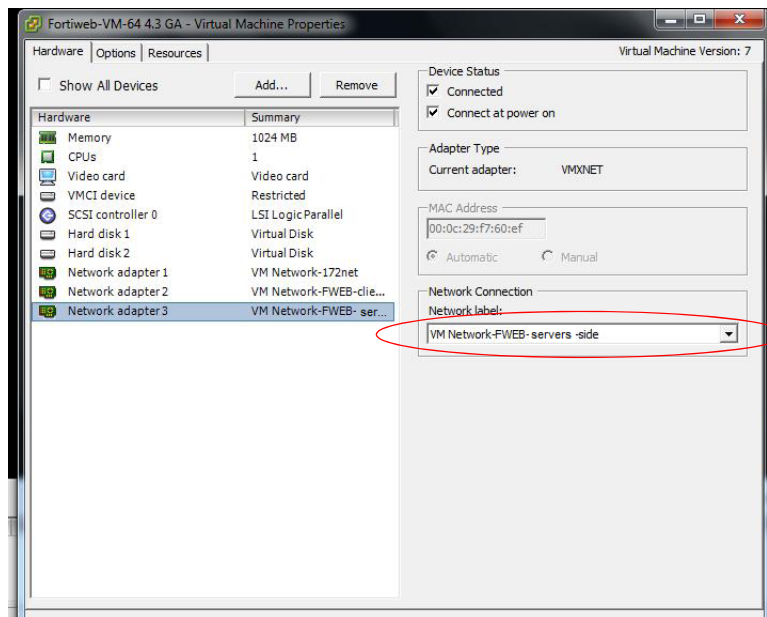
Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

### Basic Tasks

- ▶ Power on the virtual machine
- 🔧 Edit virtual machine settings

A properties window appears.



- 3 On the *Hardware* tab, select a network adapter from the hardware list.
- 4 Select the new vSwitch from the *Network label* drop-down list.
- 5 Click *OK*.

- 6 Repeat this procedure with the other vSwitch for the bridge.
- 7 Later, when configuring FortiWeb-VM, add port2 and port3, or whichever FortiWeb ports correspond to the vSwitches you created in this procedure, to the bridge (V-zone).

## Powering on the virtual appliance

Once the virtual appliance's package has been deployed and its virtual hardware configured, you can power on the virtual appliance.



**Note:** Do **not** power on the virtual appliance **unless** you have already mapped the virtual network adapter(s) ("[Mapping the virtual NICs \(vNICs\) to physical NICs](#)" on [page 27](#)). You may also want to:

- Resize disk (VMDK) (see "[Resizing the virtual disk \(vDisk\)](#)" on [page 19](#))
- Configure the number of CPUs (see "[Configuring the number of virtual CPUs \(vCPUs\)](#)" on [page 24](#))
- Set the RAM on virtual appliance ("[Configuring the virtual RAM \(vRAM\) limit](#)" on [page 25](#))

These settings cannot be configured inside FortiWeb-VM, and must be configured in the virtual machine environment.

### To power on FortiWeb-VM

- 1 On your management computer, start VMware vSphere Client.
- 2 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 3 In *User name*, type the name of your account on that server.
- 4 In *Password*, type the password for your account on that server.
- 5 Click *Login*.
- 6 In the left pane, click the name of the virtual appliance, such as *FortiWeb-VM-64-101*.

7 Click the *Getting Started* tab.

**Getting Started** Summary Resource Allocation Performance Events Console Permissions close tab X

### What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Virtual machines run on hosts. The same host can run many virtual machines.

---

### Basic Tasks

- [▶ Power on the virtual machine](#)
- [🔧 Edit virtual machine settings](#)

The diagram illustrates a virtualization architecture. A central server labeled 'Host' has a blue platform on top labeled 'Virtual Machines' containing three desktop icons. To the left, a person is shown using a laptop labeled 'vSphere Client', which is connected to the Host server.

8 Click *Power on the virtual machine*.

9 Continue with “Configuring access to the web UI & CLI” on page 37.

# Configuring access to the web UI & CLI

Once it is powered on, you must log in to the FortiWeb-VM command line interface (CLI) via the console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

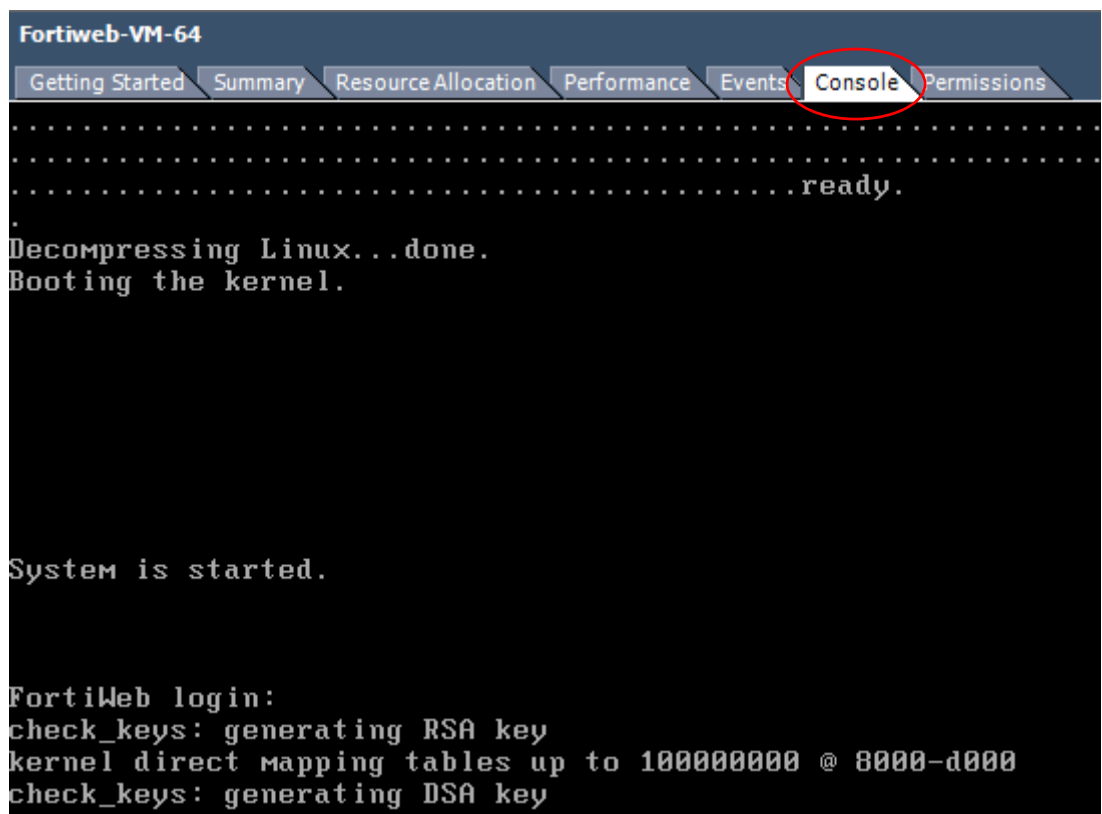
## To configure basic network settings in FortiWeb-VM

- 1 On your management computer, start VMware vSphere Client.
- 2 Log in to the VM environment.
- 3 Open the console of the FortiWeb-VM virtual appliance.

On VMware vSphere Client:

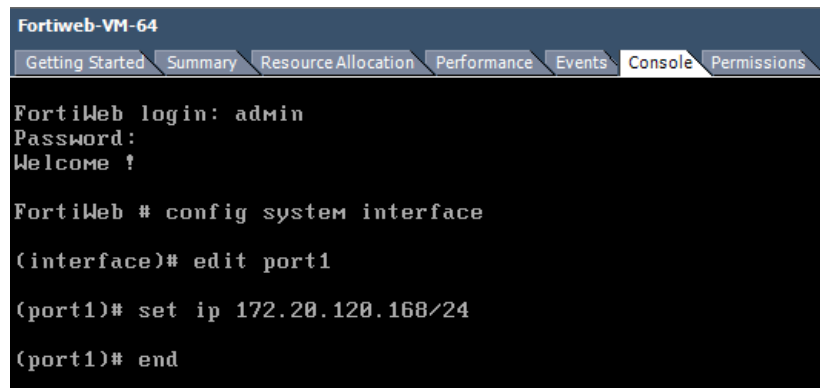
- In the left pane, select the name of the virtual appliance, such as *FortiWeb-VM-64-101*.
- Click the *Console* tab.

**Figure 4:** *Console tab in VMware vSphere Client*



- 4 At the login prompt for the local console, type:  
admin

- 5 Press Enter twice. (Initially, there is no password.)



```
Fortiweb-VM-64
Getting Started Summary Resource Allocation Performance Events Console Permissions
FortiWeb login: admin
Password:
Welcome !

FortiWeb # config system interface
(interface)# edit port1
(port1)# set ip 172.20.120.168/24
(port1)# end
```

- 6 Configure the IP address and netmask of the network interface named `port1`, or whichever network interface maps to the network physically connected to your management computer. Type:

```
config system interface
edit port1
set ip <address_ipv4> <netmask_ipv4>
end
```

where:

- `<address_ipv4>` is the IP address assigned to the network interface, such as `192.168.1.99`; the correct IP will vary by your configuration of the vNetwork (see [“Mapping the virtual NICs \(vNICs\) to physical NICs”](#) on page 27)
- `<netmask_ipv4>` is its netmask in dotted decimal format, such as `255.255.255.0`

- 7 Configure the primary and secondary DNS server IP addresses. Type:

```
config system dns
set primary <dns_ipv4>
set secondary <dns_ipv4>
end
```

where `<dns_ipv4>` is the IP address of a DNS server.

- 8 Configure a static route with the default gateway. Type:

```
config router static
edit 0
set gateway <router_ipv4>
set device port1
end
```

where `<router_ipv4>` is the IP address of the gateway router.

You should now be able to connect via the network from your management computer to `port1` of FortiWeb-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address `192.168.1.1`, go to `https://192.168.1.1/`)
- an SSH client for the CLI (e.g. If `port1` has the IP address `192.168.1.1`, connect to `192.168.1.1` on port 22.)



**Tip:** When connecting to the web UI via HTTPS, if you cannot get a connection, verify that your computer's time zone matches the appliance's configured system time. For more first-time connection troubleshooting, or instructions on how to configure the time and time zone, see the [FortiWeb Administration Guide](#).

**9** Continue by uploading the license file (see [“Uploading the license” on page 40](#)).

If you are using the 15-day free trial license and do not yet have a paid license file, you can continue instead with [“What's next?” on page 47](#).



**Note:** When the 15-day free trial license expires, you will not be able to perform any actions in the web UI until a license has been uploaded. After a valid license has been uploaded, the web UI and the CLI will be unlocked and fully functional.



**Note:** The trial period begins the first time you power on your FortiWeb-VM virtual appliance. You can upgrade the trial license to a purchased one at any time during or after the trial period by uploading the license file via the *License Information* widget in the dashboard of the web UI. For instructions, see [“Uploading the license” on page 40](#).

# Uploading the license

When you purchase a license for FortiWeb-VM, Fortinet Technical Support (<https://support.fortinet.com>) will provide a license file that you can use to convert the 15-day trial license to a permanent, paid license.

You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.



**Note:** FortiWeb-VM **requires** an Internet connection to periodically re-validate its license. It cannot be evaluated in offline, closed network environments. If FortiWeb-VM cannot contact Fortinet's FDN for 24 hours, access to the web UI and CLI will be locked.

## To upload the license via the web UI

- 1 On your management computer, start a web browser.  
Your computer must be connected to the same network as the hypervisor.
- 2 In your browser's URL or location field, enter the IP address of `port1` of the virtual appliance, such as:

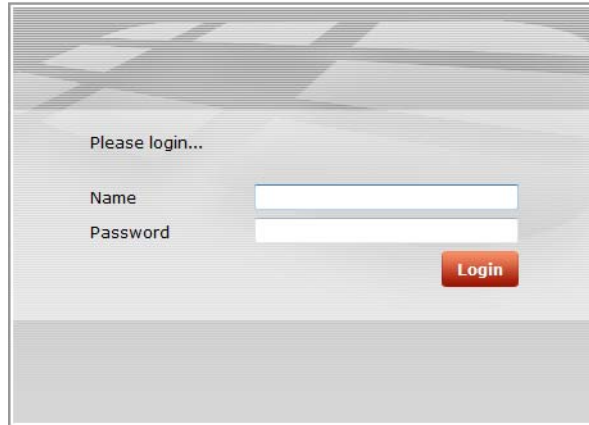
<https://192.168.1.99/>

(Remember to include the "s" in https://.)



**Note:** Initially, you must access the web UI via HTTPS. By default, HTTP is not enabled. After uploading the license, you can configure the administrative access protocols. For details, see the [FortiWeb Administration Guide](#).

Your browser connects the appliance. The web UI's login page should appear.



If you do **not** see the login page due to an SSL cipher error during the connection, and you are connecting to the trial license of FortiWeb-VM or a LENC version of FortiWeb, then your browser must be configured to accept encryption of 64-bit strength or less during the handshake. (RC2, RC4, and DES with less than 64-bit strength is supported. AES and 3DES is **not** supported in these versions.)

For example, in Mozilla Firefox, if you receive this error message:

```
ssl_error_no_cypher_overlap
```

you may need to enter `about:config` in the URL bar, then set `security.ssl3.rsa.rc4_40_md5` to `true`.

To support HTTPS authentication, the FortiWeb appliance ships with a self-signed X.509 certificate, which it presents to clients whenever they initiate an HTTPS connection to the FortiWeb appliance. When you connect, depending on your web browser and prior access of the FortiWeb appliance, your browser might display two security warnings related to this certificate:

- The certificate is not automatically trusted because it is self-signed, rather than being signed by a valid certificate authority (CA). Self-signed certificates cannot be verified with a proper CA, and therefore might be fraudulent. You must manually indicate whether or not to trust the certificate.
- The certificate might belong to another web site. The common name (CN) field in the certificate, which usually contains the host name of the web site, does not exactly match the URL you requested. This could indicate server identity theft, but could also simply indicate that the certificate contains a domain name while you have entered an IP address. You must manually indicate whether this mismatch is normal or not.

Both warnings are normal for the default certificate. SSL v3 and TLS v1.0 are supported.

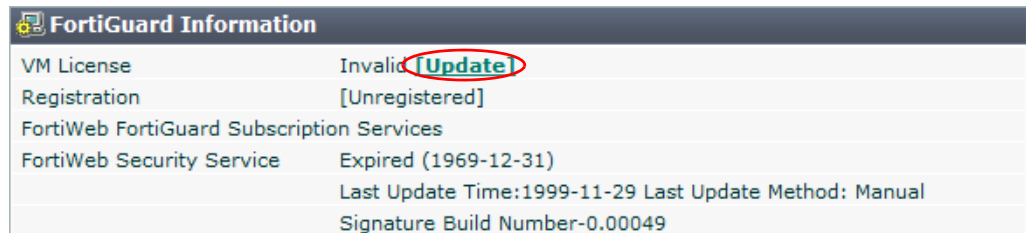
- 3 Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.

For details on accepting the certificate, see the documentation for your web browser.

- 4 In the *Name* field, type `admin`.

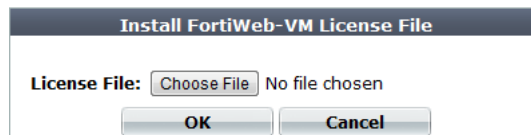
- 5 Click *Login*. (Initially, there is no password.)  
The web UI appears. The web UI initially displays its dashboard, *System > Status > Status*. The *FortiGuard Information* widget displays the current license status and contains a link where you can upload a license file.

**Figure 5: FortiGuard Information widget on System > Status > Status in the web UI before license upload**



FortiGuard Information	
VM License	Invalid <b>Update!</b>
Registration	[Unregistered]
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Expired (1969-12-31)
Last Update Time:1999-11-29 Last Update Method: Manual	
Signature Build Number-0.00049	

- 6 In the *VM License* row of the *FortiGuard Information* widget, click the *Update* link.  
The *Install FortiWeb-VM License File* dialog opens.



- 7 Depending on your browser, you may see either a *Browse* or *Choose File* button. Locate the license file (.lic) you downloaded earlier from Fortinet, then click *OK*.  
Your browser uploads the license file. Time required varies by the size of the file and the speed of the network connection. FortiWeb will then connect to Fortinet to validate its license. A message appears:

License has been uploaded. Please wait for authentication with registration servers.

- 8 Click *Refresh* on the message box.

If you uploaded a valid license, a second message box should appear, informing you that your license authenticated successfully:

License has been successfully authenticated with registration servers.

Time required varies by connectivity to the license authentication servers. If the connection does not succeed the first time, you can either wait up to 30 minutes for the next license query, or enter the CLI command:

```
exec update-now
```



**Note:** This command also contacts FortiGuard for FortiWeb Security Service contract validation and update availability.

- 9 Click *OK*.  
The web UI logs you out. The login dialog reappears.
- 10 Log in again.

- 11 To verify that the license was uploaded successfully, log in to the web UI again, then view the *License Information* widget. The *VM License* row should say *Valid*.

Also view the *System Information* widget. The *Serial Number* row should have a number that indicates the maximum number of vCPUs that can be allocated according to the FortiWeb-VM software license, such as *FVVM020000003619* (where “VM02” indicates a limit of 2 vCPUs).

If FortiWeb was also able to contact FortiGuard, its *FortiWeb Update Service* row should also indicate that the FortiGuard service contract is valid. (This second license validation may occur a minute or two after the first, and so may not appear immediately. If it does not appear, verify your DNS, network interface, and static route settings, and use `execute ping` and `execute traceroute` to verify that connectivity to the Internet is possible, and that FortiWeb can resolve domain names.)

**Figure 6:** *FortiGuard Information* widget on *System > Status > Status* in the web UI after license validation



FortiGuard Information	
VM License	Valid (Update)
Registration	cschwartz@fortinet.com
FortiWeb FortiGuard Subscription Services	
FortiWeb Security Service	Valid Contract (Expires 2013-02-05)
	Last Update Time: 2012-04-30 Last Update Method: Manual
	Signature Build Number-0.00049

<i>GUI item</i>	<i>Description</i>
<b>VM License</b>	<p>Indicates whether or not this FortiWeb-VM appliance has a paid software license. The license affects the maximum number of allocatable vCPUs.</p> <p>Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Valid</b> — The appliance has a valid, non-trial license. <i>Serial Number</i> in the <i>System Information</i> widget indicates the maximum number of vCPUs that can be allocated according to this license.</li> </ul> <p>To increase the number of vCPUs that this appliance can utilize, invalidate the current license by allocating more vCPUs in your virtual machine environment (e.g. VMware), then upload a new license. See <a href="#">“Updating the license for more vCPUs” on page 44</a>.</p> <ul style="list-style-type: none"> <li>• <b>Invalid</b> — The FortiWeb-VM appliance license either was <b>not</b> valid, <b>or</b> is currently a <b>trial</b> license.</li> </ul> <p>To upload a purchased license, click <i>Update</i>.</p> <p>This appears only in FortiWeb-VM.</p>
<b>Registration</b>	<p>Indicates which account registered this appliance with Fortinet Technical Support. Possible states are:</p> <ul style="list-style-type: none"> <li>• <b>Unregistered</b> — Not registered with Fortinet Technical Support.</li> <li>• <b>&lt;registration_email&gt;</b> — Registered with Fortinet Technical Support.</li> </ul> <p>To manage technical support or FortiGuard service contracts for this device, go to <i>System &gt; Maintenance &gt; Auto Update</i> then next to the registration email, click <i>Login</i>. A new window will appear where you can log in to the <a href="#">Fortinet Technical Support web site</a>.</p>

12 Continue with “What’s next?”.

## Updating the license for more vCPUs

If either:

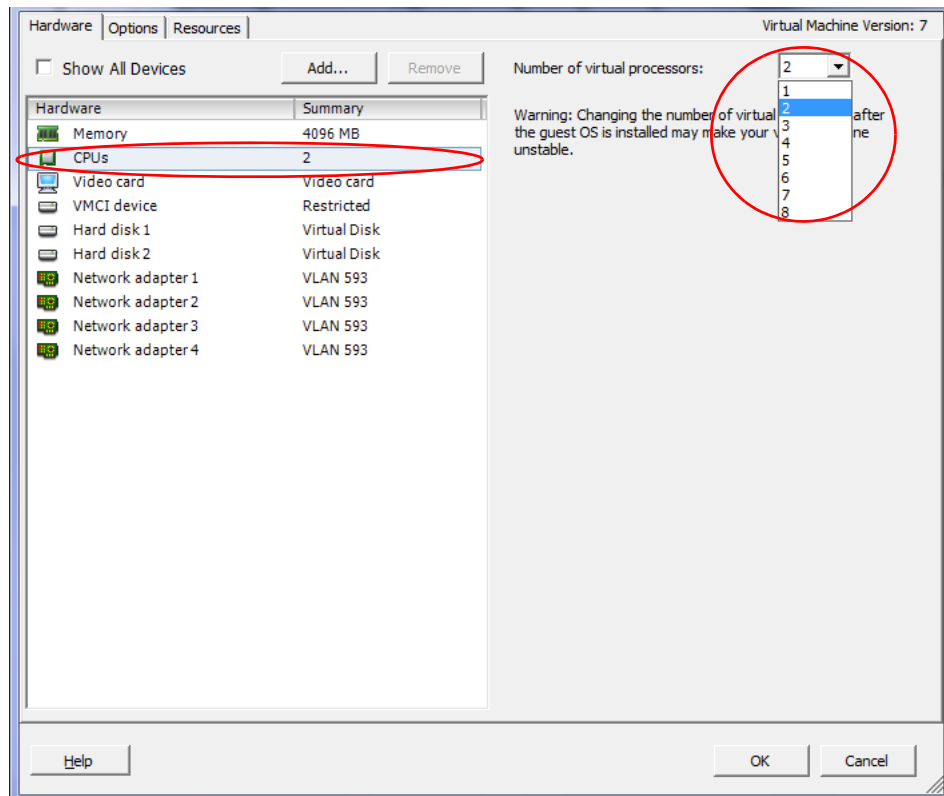
- you want to upgrade FortiWeb-VM to a license with a higher vCPU limit
- your original FortiWeb-VM license was an extended evaluation license, and you have now purchased a permanent, paid license

you must upload a new license file.

**Currently, this can only be done while the FortiWeb-VM license is invalid.** In order to upload a new license file, you must first invalidate the current one. There are multiple ways that you can do this.

### To upload a new license for more vCPUs

- 1 Log in to FortiWeb-VM as `admin` via the web UI.
- 2 Go to *System > Status > Status*.
- 3 In the *System Information* widget, click *Shut Down*.  
The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiWeb-VM, you may lose buffered data.
- 4 On your management computer, start VMware vSphere Client.
- 5 In *IP address / Name*, type the IP address or FQDN of the VMware vSphere server.
- 6 In *User name*, type the name of your account on that server.
- 7 In *Password*, type the password for your account on that server.
- 8 Click *Login*.
- 9 In the left pane, click the name of the virtual appliance, such as *FortiWeb-VM-64-101*.
- 10 Click the *Getting Started* tab.
- 11 Click *Power off the virtual machine*.
- 12 Increase the vCPU allocation. For details, see “[Configuring the number of virtual CPUs \(vCPUs\)](#)” on page 24.

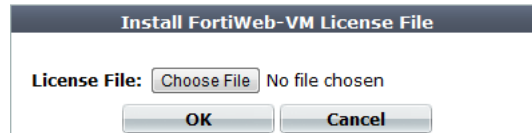


**13** Power on the virtual appliance again.

FortiWeb-VM will evaluate its current license, and discover that you have allocated an unsupported number of vCPUs, causing the current license to become invalid. This will temporarily disable most of the GUI and CLI, except for the capability to upload a new license.

**14** Log in to the web UI again.

**15** Upload the new license. For details, see [“Uploading the license” on page 40](#).



### **To upload a paid license if you have an extended evaluation**

**1** Either:

- Shut down FortiWeb-VM, power it off, then increase the number of vCPUs to invalidate the trial license. For details, see [“Configuring the number of virtual CPUs \(vCPUs\)” on page 24](#).
- Delete the instance. Re-deploy using a fresh FortiWeb-VM image with no license.
- Wait for the current evaluation period to finish, invalidating the license.

**2** Upload the new license. For details, see [“Uploading the license” on page 40](#).

# What's next?

At this point, the FortiWeb-VM virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. Before you can use FortiWeb-VM, you must configure it.

**Configure the FortiWeb-VM software using the [FortiWeb Administration Guide](#).**

After you have completed this first-time setup, you can refer to the [FortiWeb Administration Guide](#) and/or [FortiWeb CLI Reference](#). Updates, reconfiguration, and ongoing use of both FortiWeb-VM virtual appliances and physical appliance models such as FortiWeb-3000C are the same.

## Updating the virtual hardware

By default, FortiWeb-VM uses VMware virtual hardware version 5. Should you need to update your FortiWeb-VM's virtual hardware, simply be sure to shut down FortiWeb-VM before doing so.

For example, if you have a VMware ESX 4.0 environment that supports virtual hardware version 7, and you want to provide version 7 feature support such as backups to FortiWeb-VM, you would update the virtual hardware.

For more information on virtual hardware, see:

<http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675>

### To update the virtual hardware

- 1 Shut down FortiWeb-VM. To do this, you can enter the CLI command:  
`execute shutdown`
- 2 In VMware vCenter, right-click the VM and select the option to upgrade the virtual hardware.
- 3 When the upgrade is complete, power on FortiWeb-VM.

# Index

## Symbols

- \_email, 8
- \_fqdn, 8
- \_index, 8
- \_int, 9
- \_ipv4, 8
- \_ipv4/mask, 9
- \_ipv4mask, 9
- \_ipv6, 9
- \_ipv6mask, 9
- \_name, 8
- \_pattern, 8
- \_str, 9
- \_url, 8
- \_v4mask, 9
- \_v6mask, 9

## Numerics

- 3DES, 41

## A

- AES, 41
- architecture, 4
- authentication, 41
  - license, 5, 42

## B

- backup, 47
- bit strength, 41
- bridge, 27, 29
- browser
  - warnings, 41

## C

- certificate
  - authority (CA), 41
  - default, 41
  - mismatch, 41
  - self-signed, 41
  - warning, 41
- CIDR, 9

- command line interface (CLI), 7
- common name (CN), 41
- console, 37
- conventions, 6

## D

- default
  - certificate, 41
  - IP address, 38
  - password, 42
- DES, 41
- documentation
  - conventions, 6
- domain name
  - certificate, 41
- dotted decimal, 9
- dvSwitch, 30

## E

- encryption
  - weak, 41
- Error 113, 41
- ERROR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH, 41
- expected input, 7

## F

- Firefox, 41
- FortiGuard
  - services, 11
- Fortinet
  - Distribution Network (FDN), 5, 40
  - Technical Documentation
    - conventions, 6
  - Technical Support, 11
  - Technical Support, registering with, 11
- FortiWeb-VM, 41
- fully qualified domain name (FQDN), 8

## G

- gateway, 38
- guidelines, 19

## H

- handshake, 41
- hardware abstraction layer (HAL), 10
- host name, 41
- HTTPS, 41
- hypervisor, 10

## I

- index number, 8
- input constraints, 7
- installation, 6
- IP address, 38, 41
  - private network, 6

## L

- license, 11, 41
  - CPUs, 24
  - file, 5, 42
  - query, 5, 42
  - status, 42
  - trial, 5
  - upload, 42
- locked, 5, 40
- low encryption (LENC), 41

## M

- management computer, 10
- message box, 42
- Mozilla
  - Firefox, 41

## N

- netmask, 38
- network
  - interface, 38
  - mapping, 18
- NFS, 19

## O

- operation mode, 27

## P

- password, 42
- pattern, 8
- performance, 10, 26
- port1, 38, 40

- product registration, 11
- promiscuous mode, 30, 32
- proxy
  - true transparent, 27

## Q

- query
  - license, 5, 42

## R

- RC2, 41
- RC4, 41
- registration
  - number, 5
  - servers, FDN, 5, 42
  - with Fortinet Technical Support, 11
- regular expression, 8
- resource pool, 17
- RFC
  - 1918, 6
- route
  - static, 38
- router, 38

## S

- security certificate, 41
- self-signed, 41
- sizing guidelines, 19
- SSH, 38
- SSL
  - version, 41
- ssl\_error\_no\_cypher\_overlap, 41
- static route, 38
- storage repository, 19
- string, 9
- syntax, 7

## T

- time zone, 39
- TLS
  - version, 41
- transparent, 27
- trial, 5
  - license, 41
- trust certificate, 41

## U

- upload, 42
- URL, 41

## V

- value parse error, 8
- vDisk, 19
- version
  - SSL/TLS, 41
  - supported hypervisor, 10
- virtual
  - machine, 10
  - machine disk format (VMDK), 19
- virtual machine, 10
- virtualization, 6
- vSwitch, 18, 27

V-zone, 29

## W

- web browser, 38
  - warnings, 41
- wild cards, 8

## X

X.509, 41



## FortiWeb-VM 4.0 MR3 Patch 7 Install Guide

8 May 2012 • 1st Edition

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance 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 the performance metrics herein. 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 guarantees. 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.

<b>Technical Documentation</b>	<a href="http://docs.fortinet.com">http://docs.fortinet.com</a>
<b>Knowledge Base</b>	<a href="http://kb.fortinet.com">http://kb.fortinet.com</a>
<b>Forums</b>	<a href="http://support.fortinet.com/forum">http://support.fortinet.com/forum</a>
<b>Training</b>	<a href="http://training.fortinet.com">http://training.fortinet.com</a>
<b>Technical Support</b>	<a href="https://support.fortinet.com">https://support.fortinet.com</a>

Please report errors or omissions to:  
[techdoc@fortinet.com](mailto:techdoc@fortinet.com)