

# Walled garden for on-boarding user devices to eduroam

## Technical Deployment Guide

## Contents

Walled garden for onboarding user devices to eduroam .....	1
Background .....	1
Considerations .....	2
Preparing .....	4
Creating a VMware Virtual Machine for pfSense .....	5
Uploading the ISO Image .....	15
Attaching ISO Image to the VM .....	20
pfSense Installation .....	23
Configuring pfSense .....	35
Adding a LAN Interface .....	45
VMWare ESXi Networking Configuration .....	45
Virtual Machine Networking Configuration .....	50
Adding the interface into pfSense .....	53
Captive Portal configuration .....	60
Installing Open VM Tools .....	70
Access Point configuration .....	78
Testing the user experience .....	79

## Background

One of the key barriers in successful deployment of eduroam, is around ensuring that users are adequately supported. 802.1x/WPA2 Enterprise configuration on the majority of devices is a little more complex than PSK-based Wireless solutions, which users are familiar with at home. As a result there is a need for on-boarding tools to be made available to users, such as eduroam CAT.

Organisations providing eduroam will need to provide access to their chosen on-boarding tool; typically they will be available via the organisations eduroam support web page. The challenge for many organisations is that devices need Internet access to visit to the organisations eduroam support web page, this usually isn't a problem for mobile phones which usually have access to the Internet via the mobile network.

However, there are other situations which require an Internet connection or local network access to gain access to the on-boarding tools. This includes where organisations have poor mobile coverage, but also for tablets and laptop devices, which may not have access to the mobile network.

The solution deployed by many organisations is that of a 'Walled Garden', this is a network connection that enables sufficient access to download on-boarding tools, gain access to support webpage and any other relevant access, but it should fall short of providing full internet access.

Our work with the Further Education sector has highlighted the need for organisations deploying eduroam to also deploy a 'Walled Garden' to on-board large numbers of users onto eduroam, and to enable users to 'self-service'. The 'Walled Garden' is typically made available by broadcasting an open wireless SSID.

The following guide is aimed to help you in configuring a walled garden network. This uses the Open-source product pfSense, which is a Firewall solution based on FreeBSD. It's a viable solution, even for organisations which typically don't use Unix-based operating systems, since it is almost entirely configured through a web page, is comparable to appliance-based solutions, and is relatively easy to maintain and update.

pfSense can be configured to run in a Virtual Machine, this guide covers using VMware, but it can also be deployed in a Xen environment, or on physical hardware.

Since the completion of this guide, there has been an update to pfSense from 2.2 to 2.3, and has is now known as the pfSense Community Edition. Since the update the user interface has improved, but there is very little change to the menu options and pages. These instructions have been tested with version 2.2.4 and 2.3.2, we recommend using the latest stable version of the software.

Author: **Jon Agland**, Subject specialist (network technologies and infrastructure), Jisc

Document - Version 0.5

Date 9<sup>th</sup> August 2016

## Changelog

Version	Modification	Author	Date
0.2	Initial version	Jon Agland	19 <sup>th</sup> January 2016
0.3	Updating following feedback from eduroam (UK) team	Jon Agland	20 <sup>th</sup> April 2016
0.4	Added eduroam CAT website list	Jon Agland	6 <sup>th</sup> July 2016
0.5	Update Background related to new pfSense 2.3 release Added missing Network screenshot from Create New Virtual Machine Changelog added	Jon Agland	9 <sup>th</sup> August 2016

## Considerations

You should take some time to consider and even design the solution, security is one of the key areas to think about. Opening up an open wireless network is a significant risk. Whilst we have some confidence that pfSense can provide a secure solution, you may wish to consider additional safeguards. We would suggest the following

- LAN port of pfSense must be into a dedicated network (VLAN)
  - VLAN should have no IP address on other Routers, Switches, Firewall
  - DHCP/IP Helper/Directed-Broadcast is not required, DHCP will be provided by pfSense
  - VLAN may need IP addressing (an SVI) on the Wireless controller
    - We know this to be true for Wireless controllers from Cisco and Meru.
  - If you need multiple controllers at different locations, which then use different VLANs, then you may need multiple pfSense units
  - This VLAN will be your 'walled garden' where untrusted devices will be connected.
  - The IP subnet used should be unique on your network
- WAN port of pfSense
  - Should be into a dedicated network (VLAN)
  - Could be a 'DMZ', restricted network, or the perimeter/Internet edge network
  - Ensure that pfSense Web and SSH interfaces are secured appropriately.
  - The corresponding IP interface e.g. on a Router, Layer 3 Switch or Firewall, should have an appropriate Access-List to offer further protection to your infrastructure
  - Consider that a failure or misconfiguration of the pfSense could expose this network to untrusted devices.
  - The IP subnet used must be unique on your network, and be routable out the Internet but can utilise NAT
- Further usage of pfSense;
  - You could utilise to provide a Captive Portal for non-eduroam users
    - Janet connected sites should consider our guidance on **guest and public access**.
  - If using dynamic VLANs in your eduroam/RADIUS configuration, your 'walled-garden' could be elected as the default VLAN for the controller or for RADIUS in the event of a configuration issue.
  - A separate network and interface could be used to provide the eduroam visitor network, this will need to be compliant with the **eduroam (UK) Technical Specification**.

## Preparing

Start by downloading the latest ISO image from the pfSense website. Whilst a 32-bit version is available for most installations you should use the 64-bit version.

The pfSense ISO image is compressed using gzip, therefore you may need a package such as 7Zip or you could gunzip the file on a Linux/Unix system.

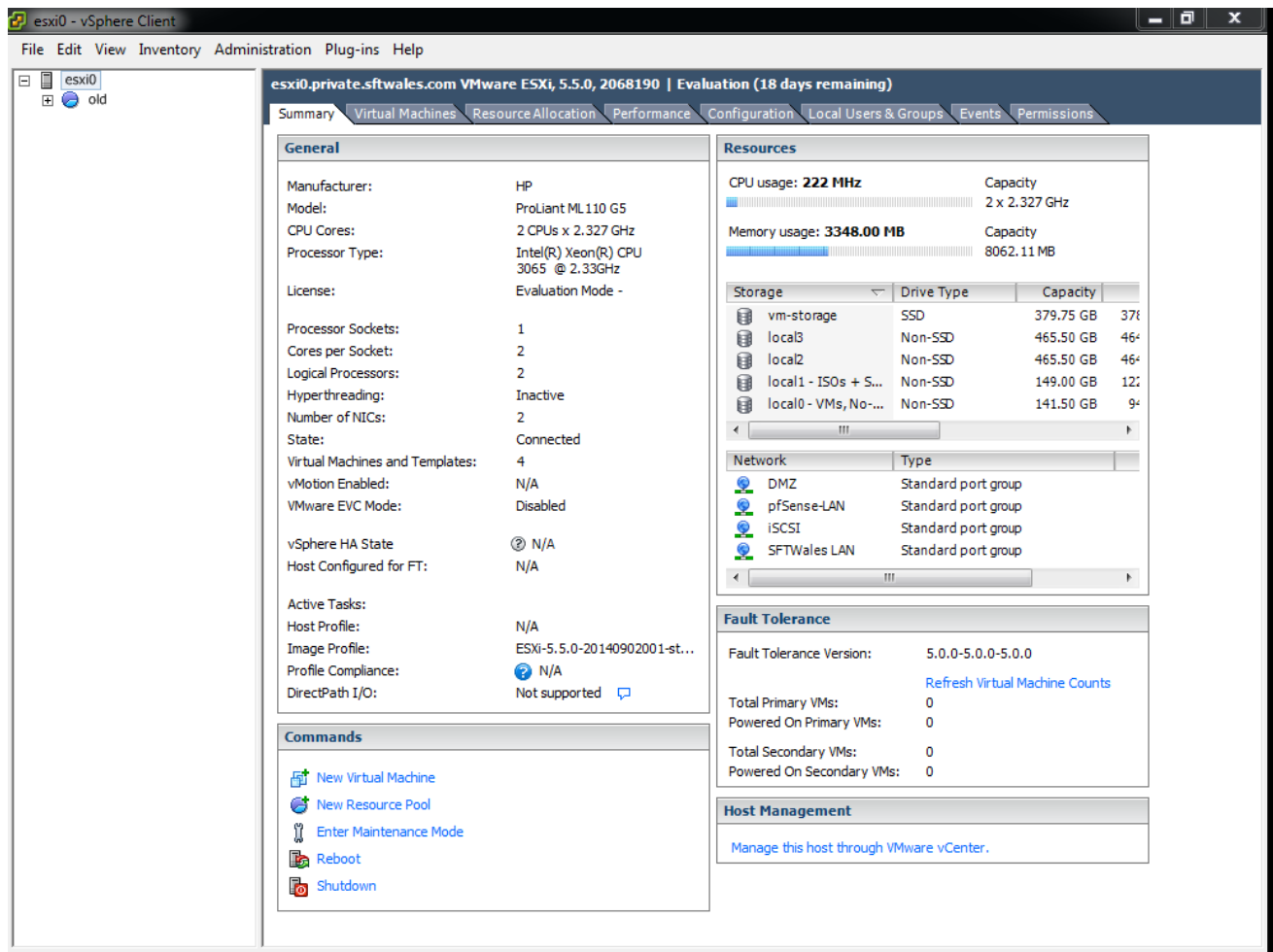
Download the Captive Portal PHP code from [Gist/Github](#).

RAW PHP version for download ([RAW PHP version of file](#))

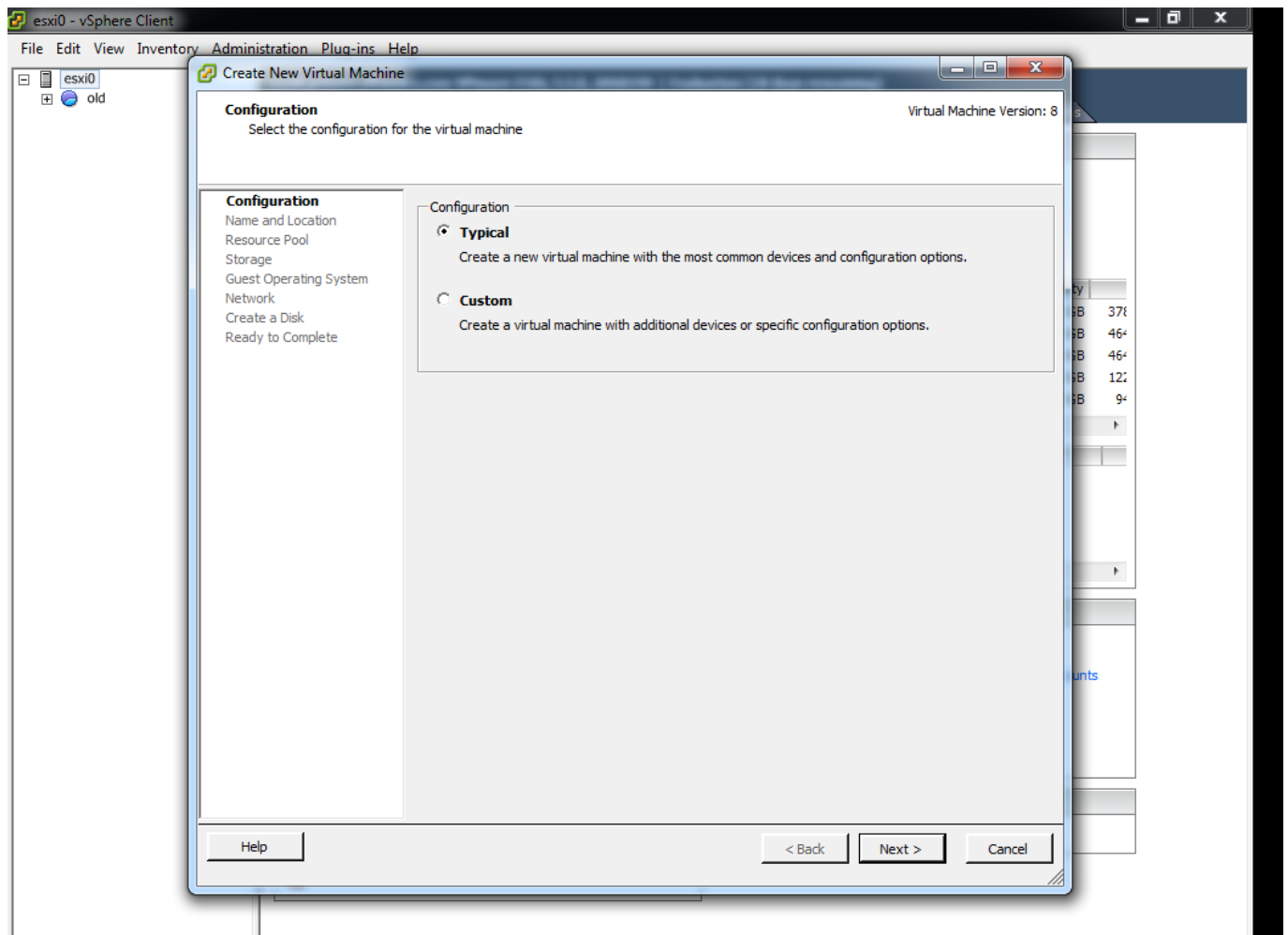
Code version for info/comment/contribution ([Gist/Github of captiveportal.php](#))

# Creating a VMware Virtual Machine for pfSense

Open up your VMware vSphere Client, Right click on your Host/Cluster/Resource Pool and choose 'New Virtual Machine'

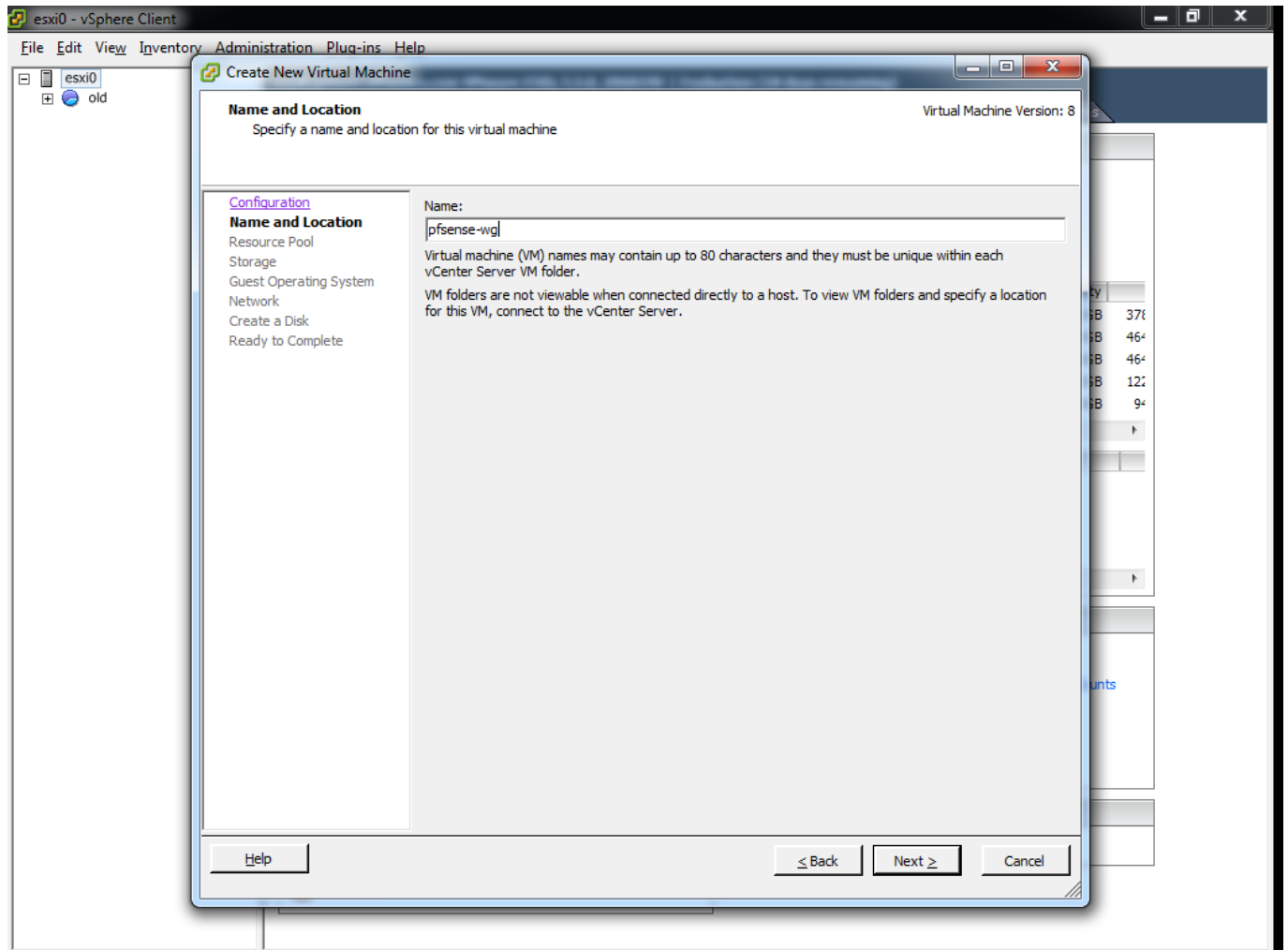


## Choose Typical

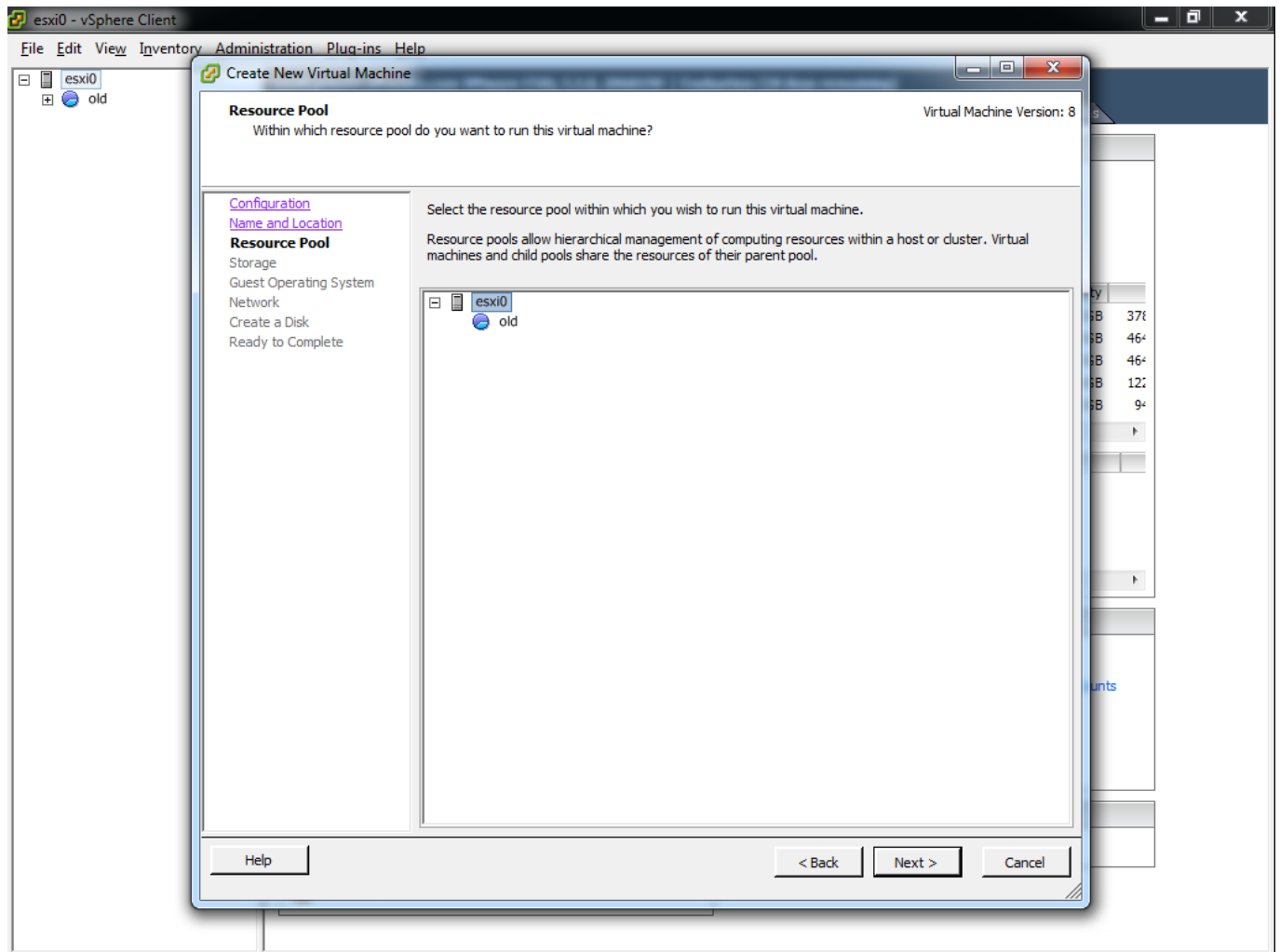




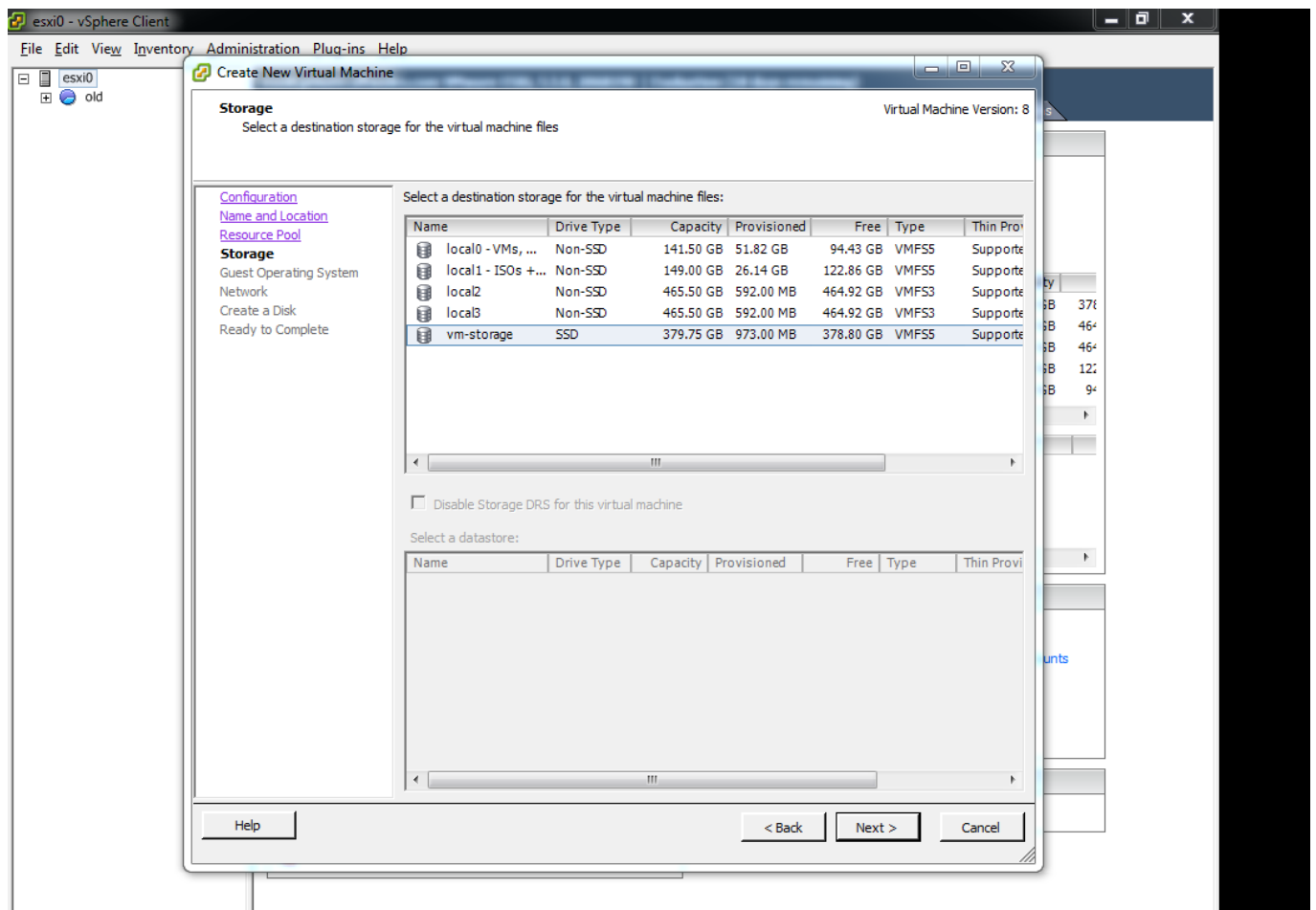
Enter a name for your virtual machine (in this instance we chose pfsense-wg)



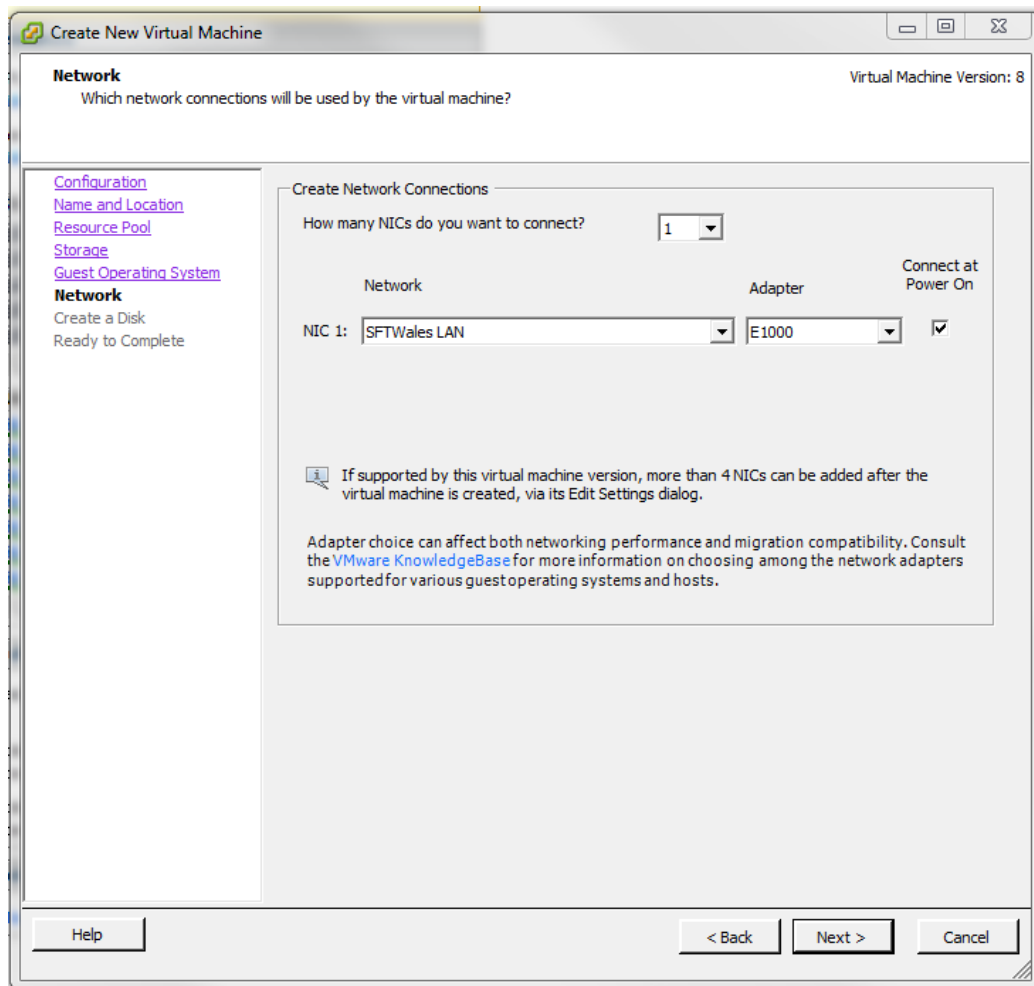
Choose the Resource Pool and click Next;



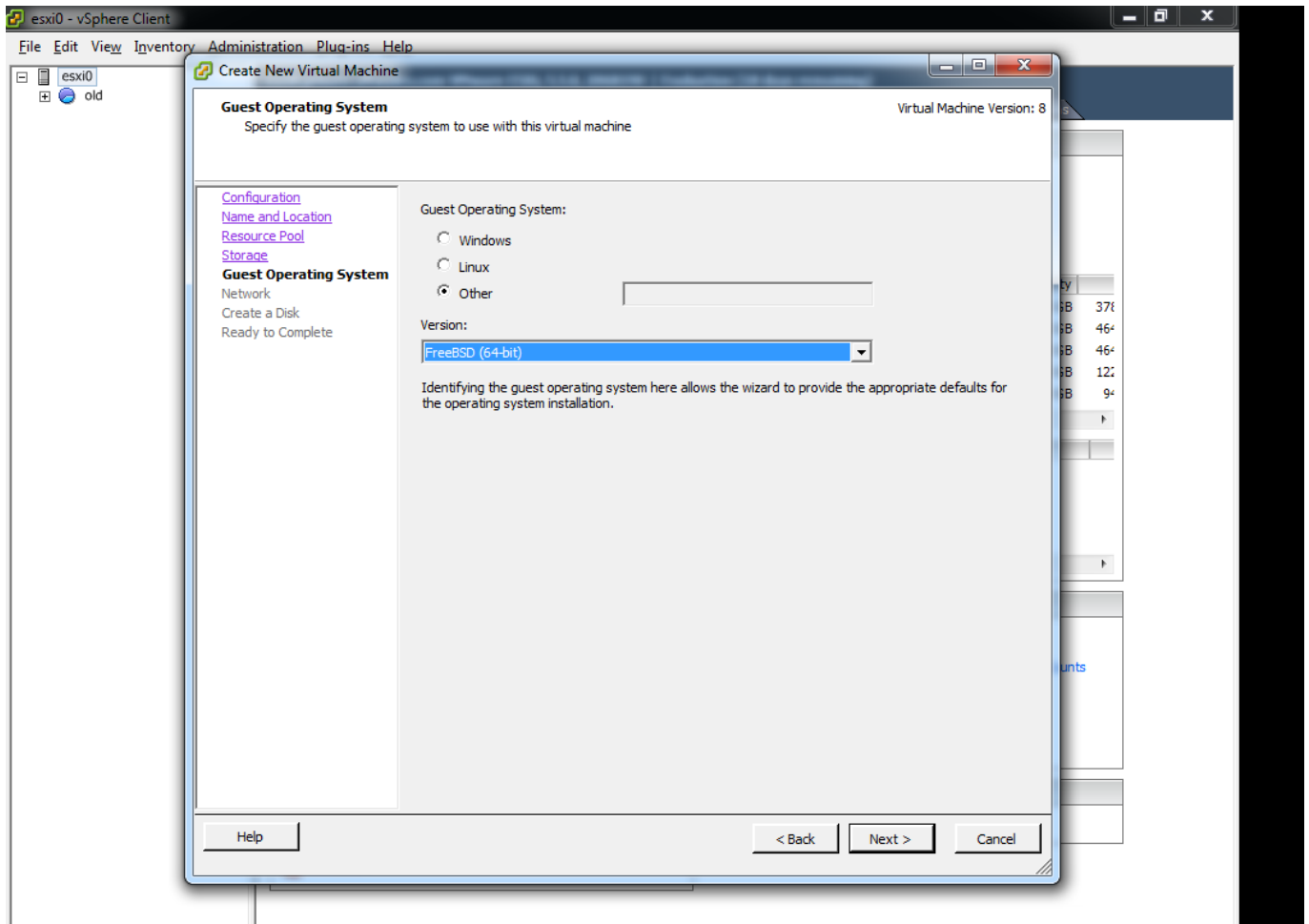
Choose an appropriate storage location. In most environments a SAN or NAS are used, rather than local disks, you will require ~8GB of storage to start. The storage needn't be your Highest Tier (e.g.. SSD/SAS), Lower Tier storage (e.g. SATA) will be more than sufficient for most usage.



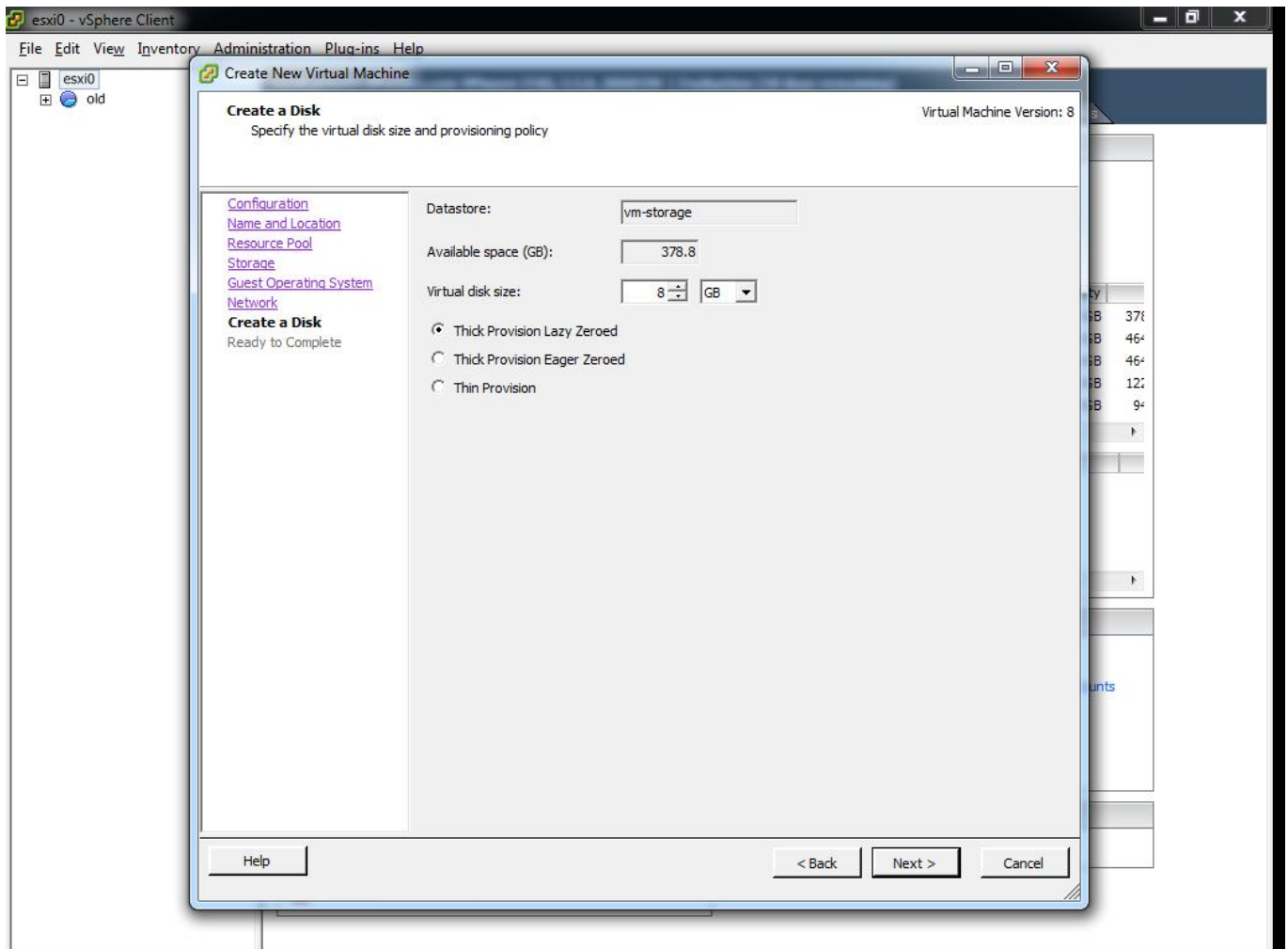
Choose the number of network interfaces and their connections, at this stage choose just one interface for example on a LAN or DMZ. At a later stage we will add an additional interface for the 'Walled Garden', do not add it now.



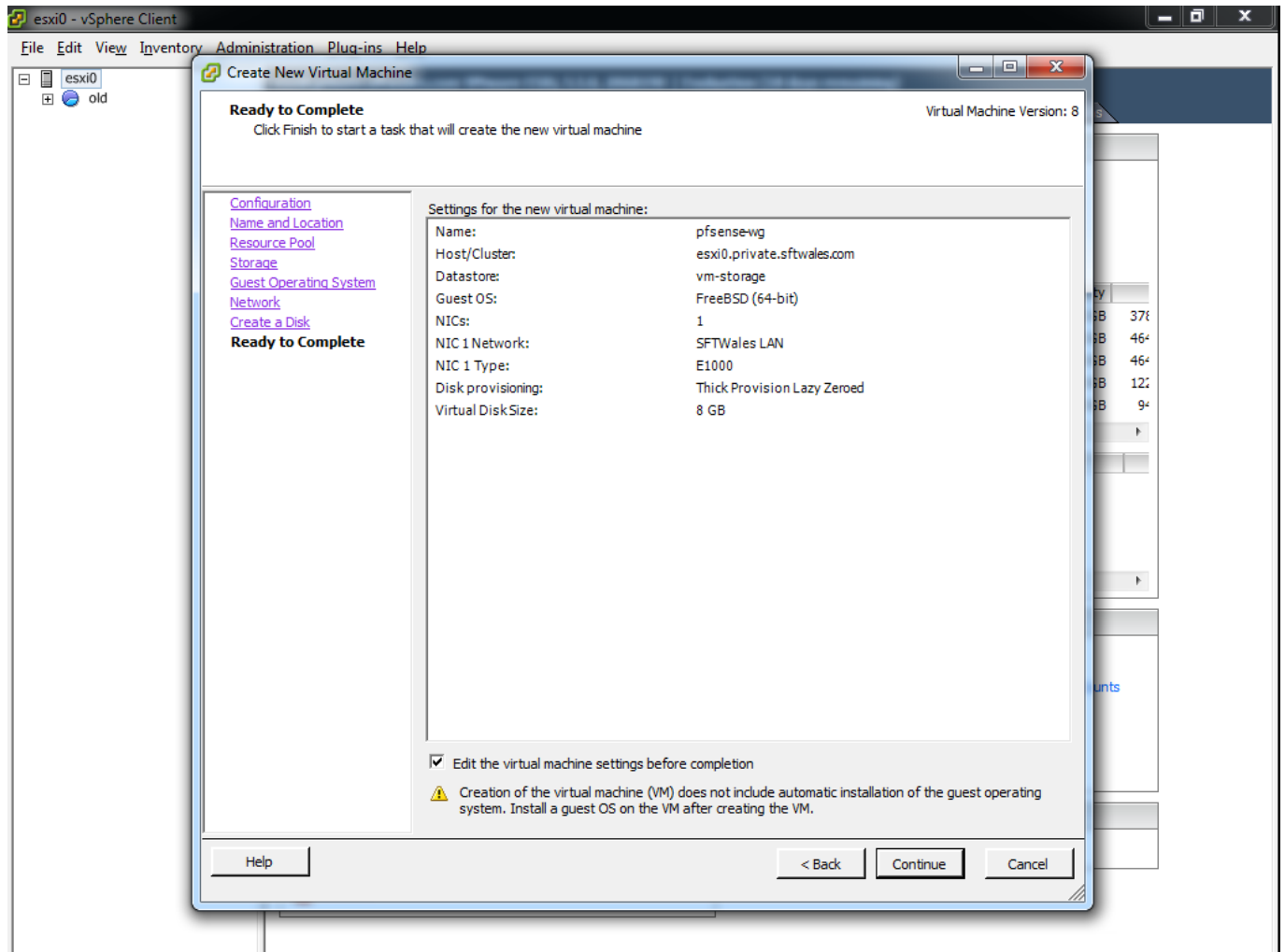
Choose the Guest Operating System version (FreeBSD 64-Bit)



Select the size of the disk. This can remain at the default of 8GB. The type i.e. Thick Provision or Thin Provision will depend on your procedures;

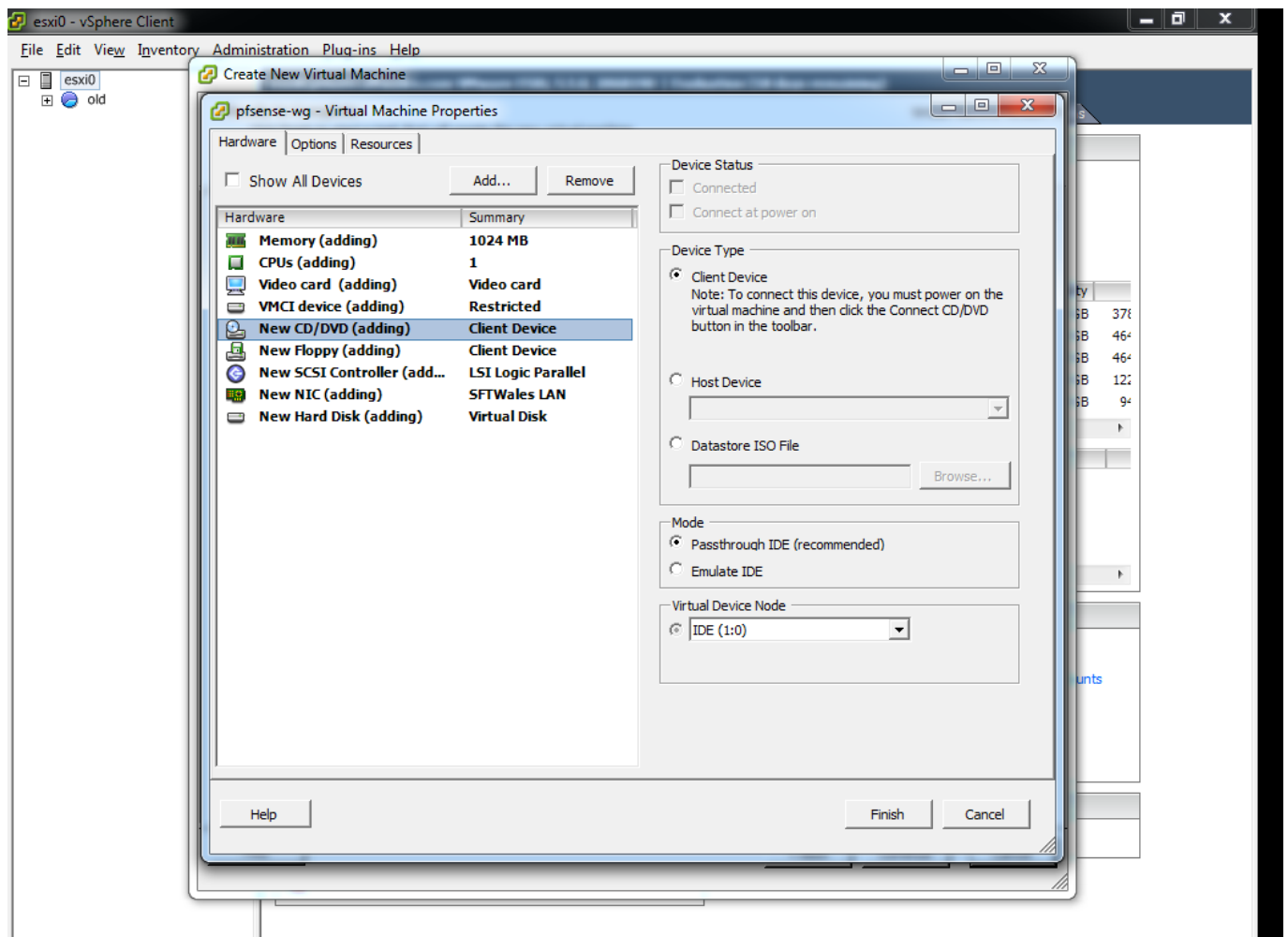


On this screen, remember to tick 'Edit the virtual machine settings before completion'



Complete the following changes

- Memory - adjust as required (for small installations 256MB may be suitable).
- CPUs – adjust as required (for most installations 1 CPU will be sufficient)
- Floppy – can be removed
- NIC – Check that the Interface is set correctly, this will become the 'WAN Interface' within pfSense.





## Uploading the ISO Image

Choose a Datastore under Storage, Right click and choose 'Browse Datastore'

The screenshot shows the vSphere Client interface for an ESXi host named 'esxi0'. The left sidebar shows the host 'esxi0' under the 'old' datacenter. The main pane displays the 'Configuration' tab for the host 'esxi0.private.sftwales.com VMWare ESXi, 5.5.0, 2068190 | Evaluation (18 days remaining)'. The 'General' tab is selected, showing host details like Manufacturer (HP), Model (ProLiant ML110 G5), CPU Cores (2 CPUs x 2.327 GHz), Processor Type (Intel(R) Xeon(R) CPU 3065 @ 2.33GHz), License (Evaluation Mode -), Processor Sockets (1), Cores per Socket (2), Logical Processors (2), Hyperthreading (Inactive), Number of NICs (2), State (Connected), Virtual Machines and Templates (4), vMotion Enabled (N/A), VMware EVC Mode (Disabled), vSphere HA State (N/A), Host Configured for FT (N/A), Active Tasks (N/A), Host Profile (N/A), Image Profile (ESXi-5.5.0-20140902001-st...), Profile Compliance (N/A), and DirectPath I/O (Not supported). The 'Resources' tab shows CPU usage (222 MHz), Memory usage (3348.00 MB), and a table of storage devices. The 'Commands' tab lists actions like 'New Virtual Machine', 'New Resource Pool', 'Enter Maintenance Mode', 'Reboot', and 'Shutdown'. The 'Fault Tolerance' tab shows Fault Tolerance Version (5.0.0-5.0.0-5.0.0) and counts for Primary and Secondary VMs. The 'Host Management' tab shows a link to 'Manage this host through VMware vCenter'.

**General**

Manufacturer: HP  
Model: ProLiant ML110 G5  
CPU Cores: 2 CPUs x 2.327 GHz  
Processor Type: Intel(R) Xeon(R) CPU 3065 @ 2.33GHz  
License: Evaluation Mode -  
Processor Sockets: 1  
Cores per Socket: 2  
Logical Processors: 2  
Hyperthreading: Inactive  
Number of NICs: 2  
State: Connected  
Virtual Machines and Templates: 4  
vMotion Enabled: N/A  
VMware EVC Mode: Disabled  
vSphere HA State: N/A  
Host Configured for FT: N/A  
Active Tasks: N/A  
Host Profile: N/A  
Image Profile: ESXi-5.5.0-20140902001-st...  
Profile Compliance: N/A  
DirectPath I/O: Not supported

**Resources**

CPU usage: 222 MHz Capacity: 2 x 2.327 GHz  
Memory usage: 3348.00 MB Capacity: 8062.11 MB

Storage	Drive Type	Capacity
vm-storage	SSD	379.75 GB
local3	Non-SSD	465.50 GB
local2	Non-SSD	465.50 GB
local1 - ISOs + S...	Non-SSD	149.00 GB
local0 - VMs, No...	Non-SSD	141.50 GB

**Network**

Network	Type
DMZ	Standard port group
pfSense-LAN	Standard port group
iSCSI	Standard port group
SFTWales LAN	Standard port group

**Commands**

- New Virtual Machine
- New Resource Pool
- Enter Maintenance Mode
- Reboot
- Shutdown

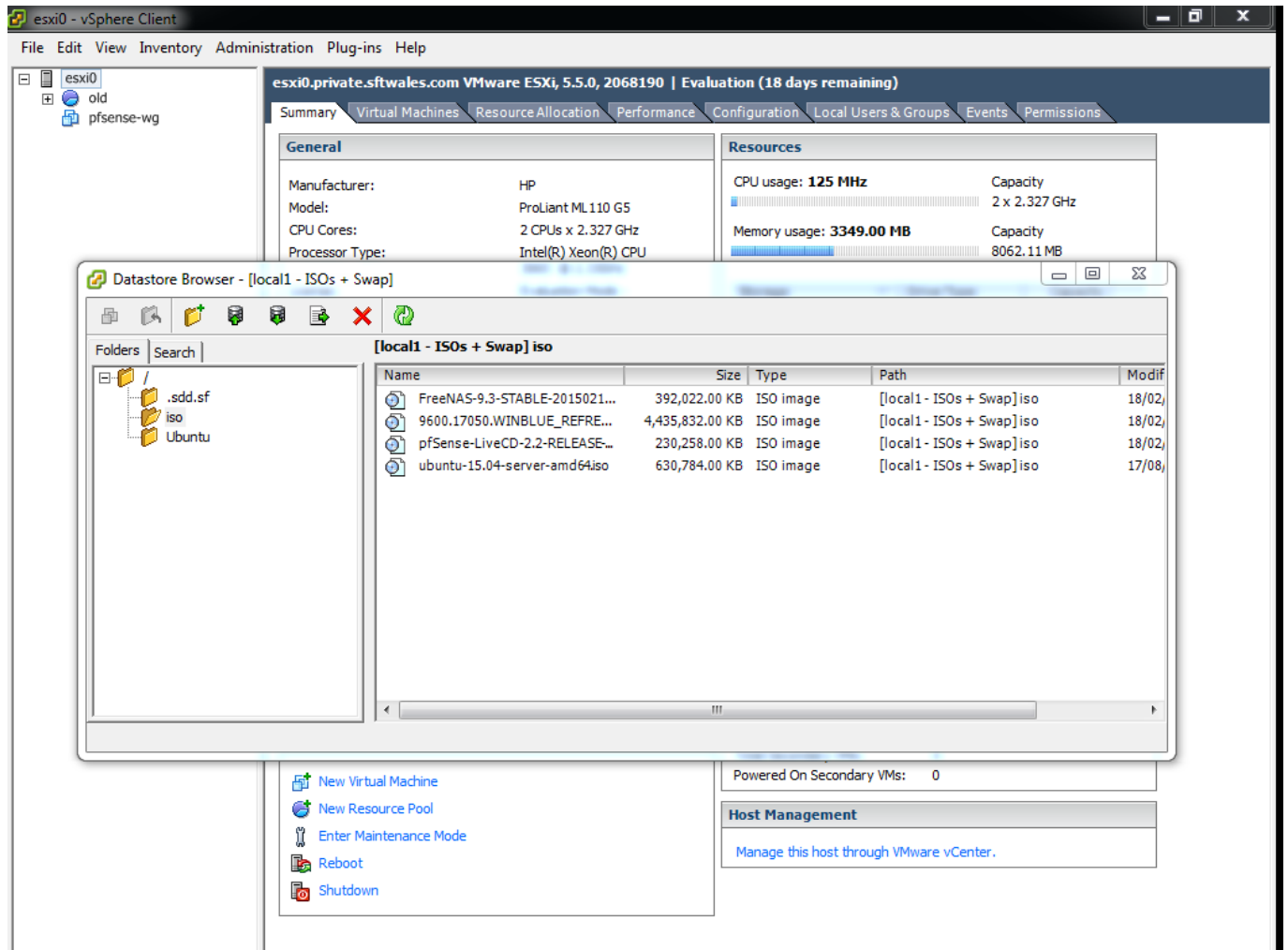
**Fault Tolerance**

Fault Tolerance Version: 5.0.0-5.0.0-5.0.0  
Total Primary VMs: 0  
Powered On Primary VMs: 0  
Total Secondary VMs: 0  
Powered On Secondary VMs: 0

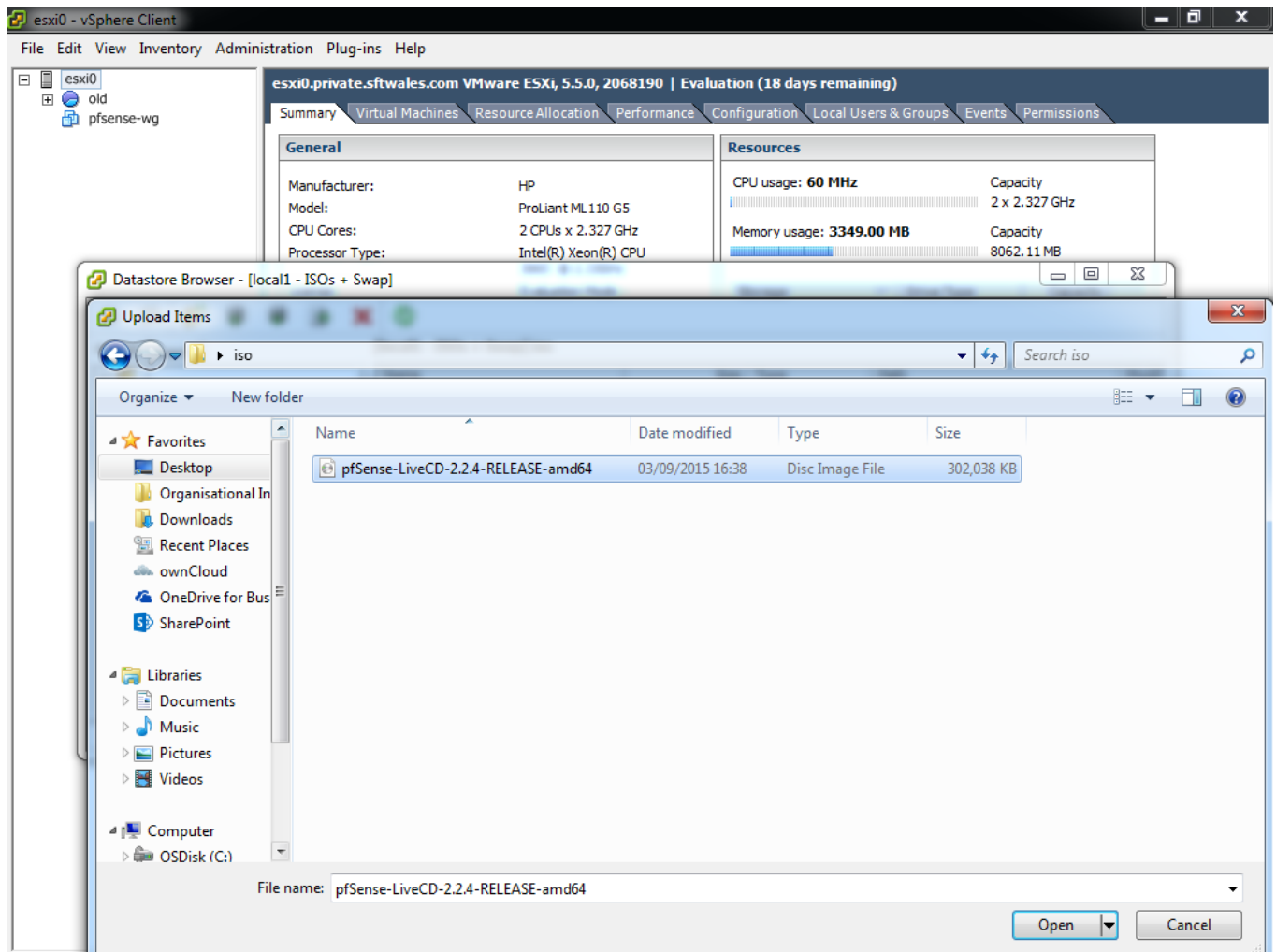
**Host Management**

Manage this host through VMware vCenter.

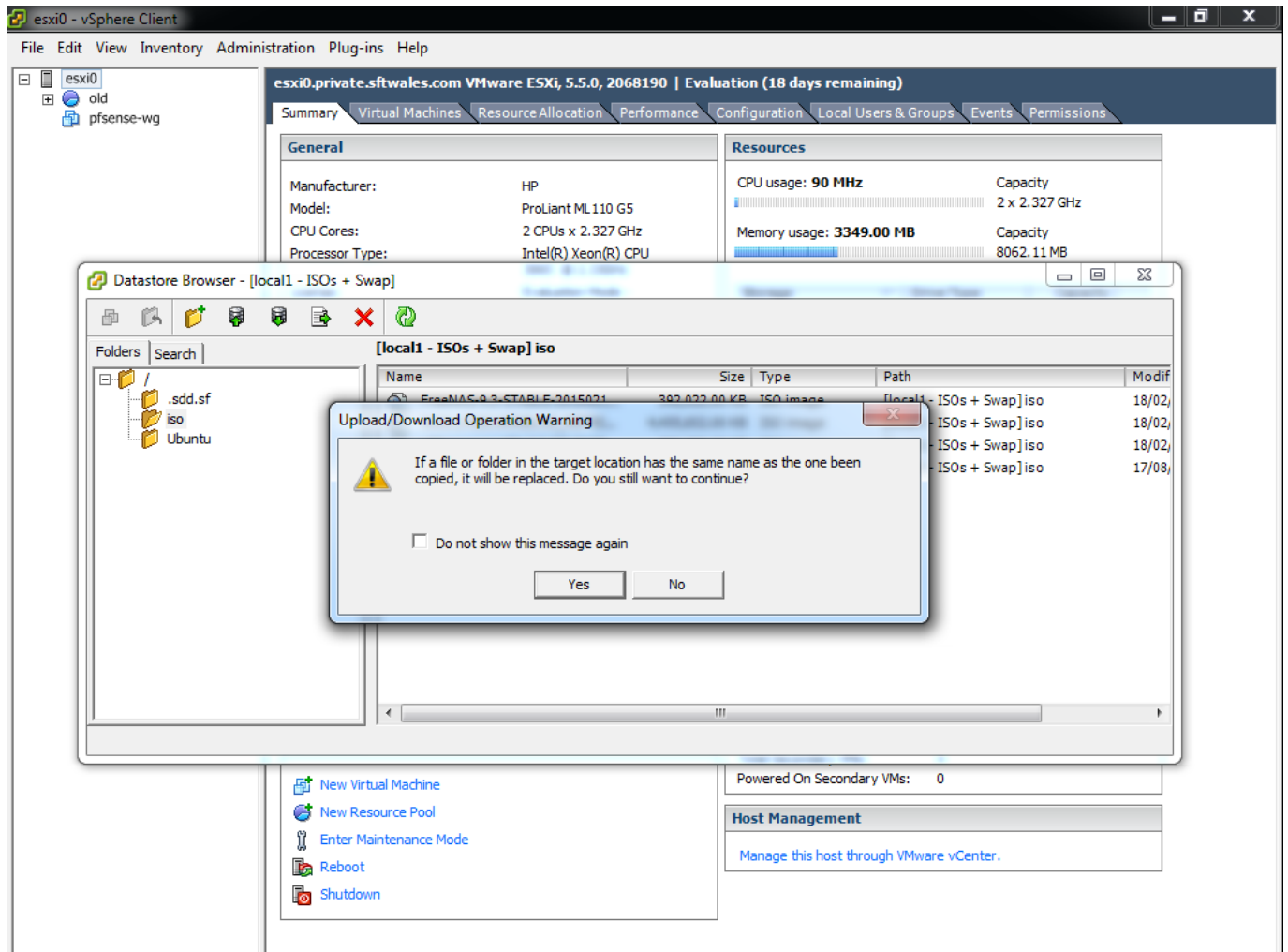
Next click on the 'Upload files to Datastore' icon (It's the one with the green arrow point upwards)



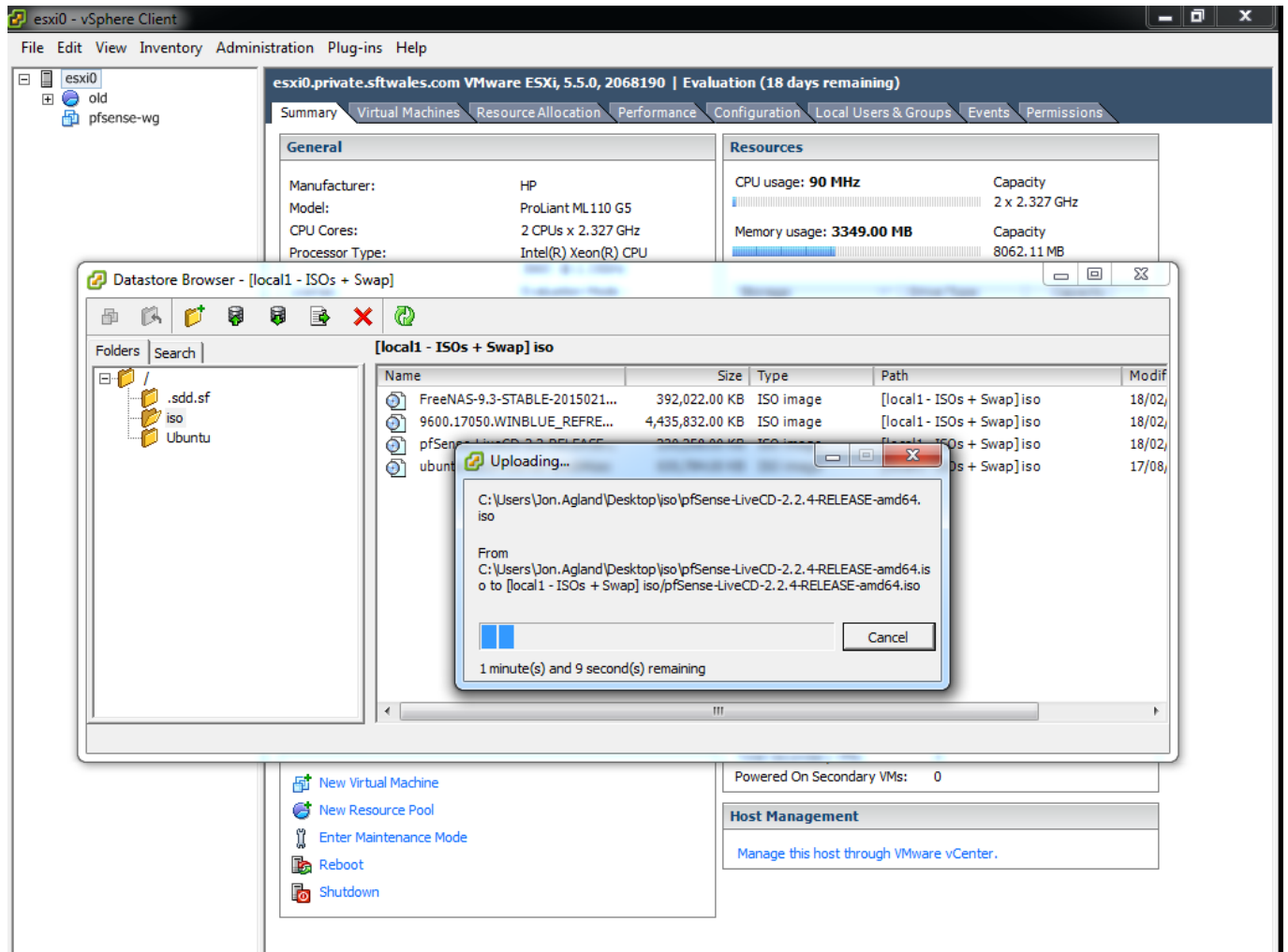
Next choose the ISO image you wish to upload (If you do not have an ISO image refer to the pre-requisites section)



On the following dialogue you can select 'Yes'

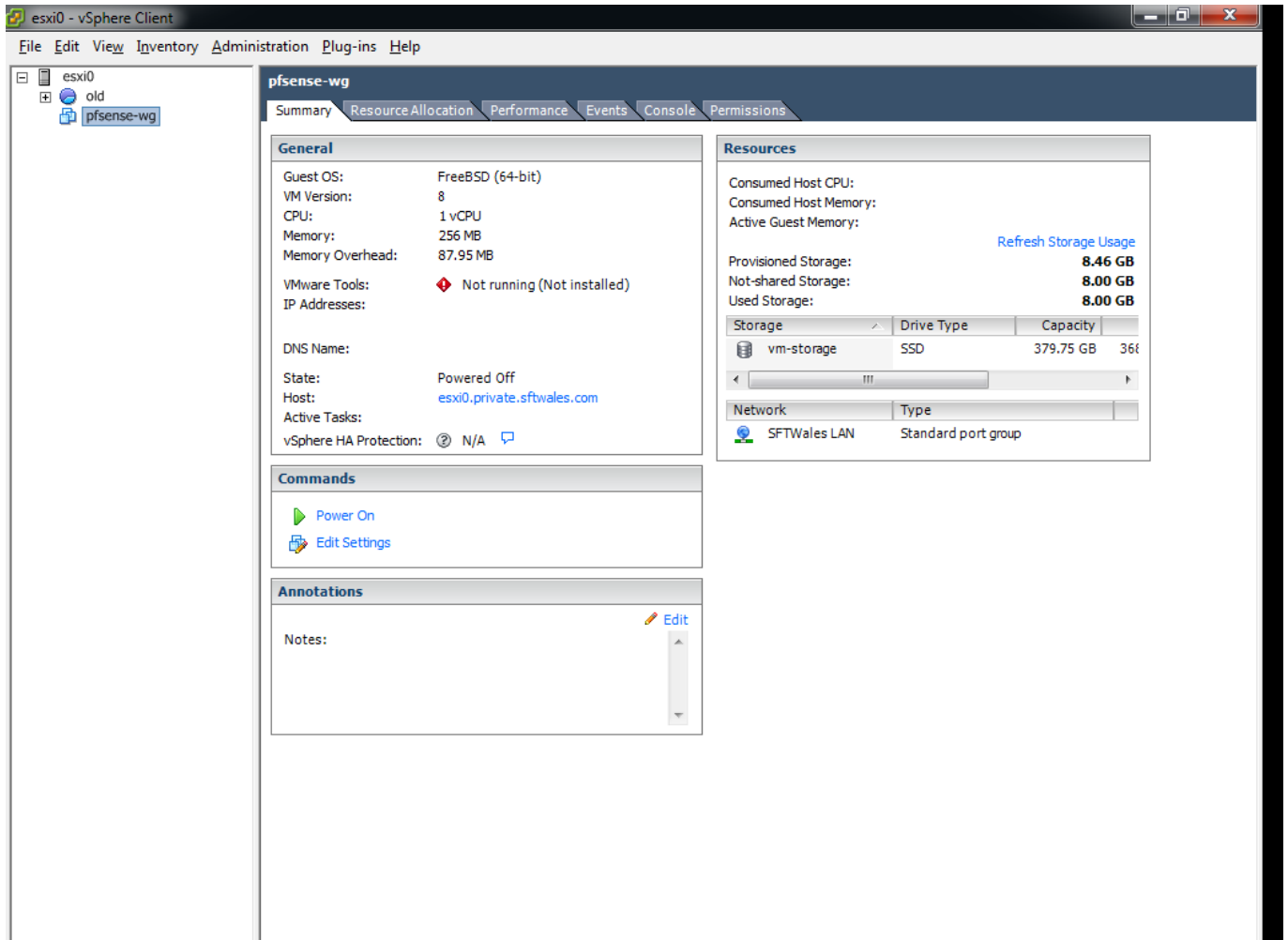


The file may take a few minutes to upload (depending on network and storage performance)

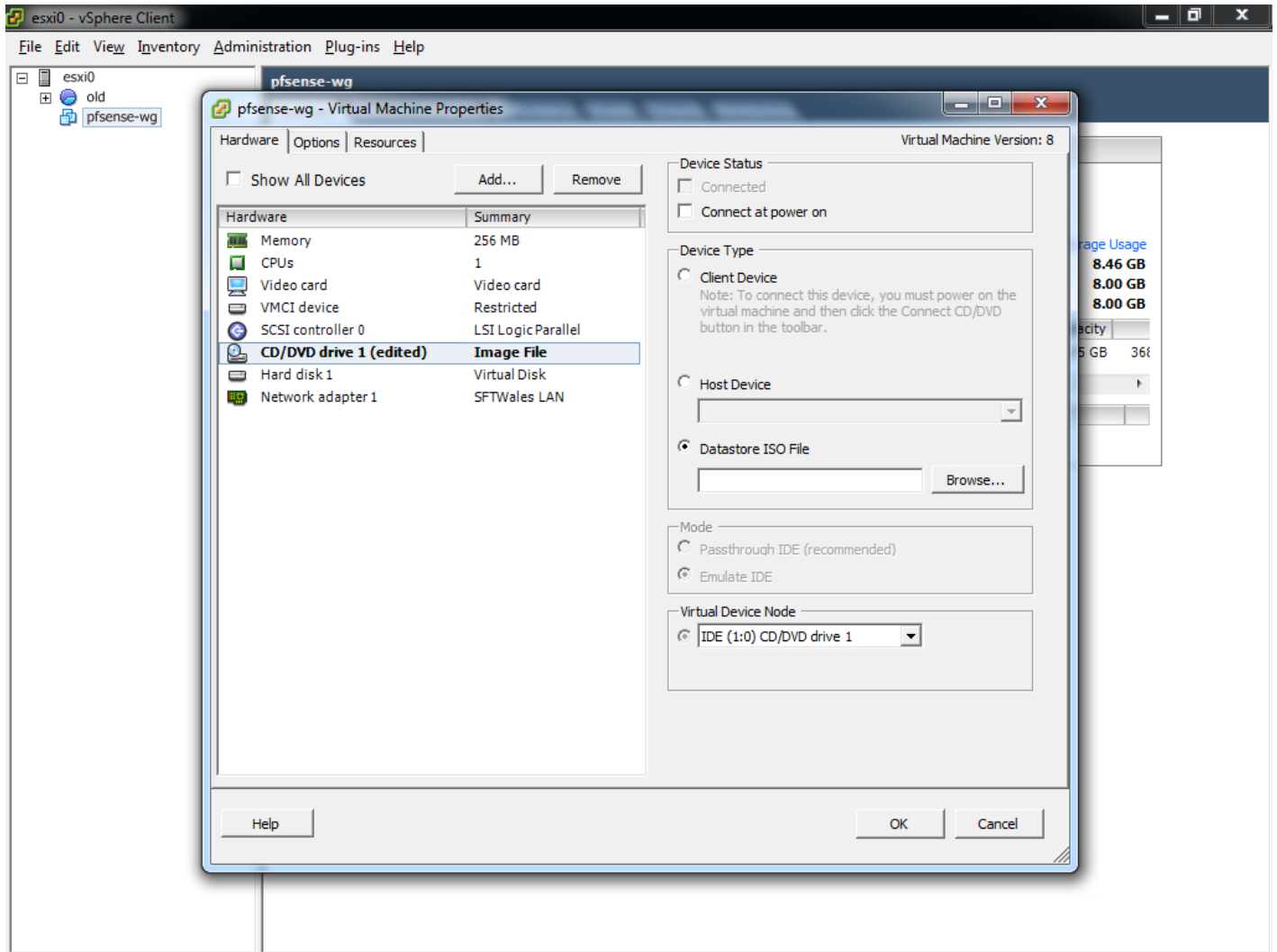


## Attaching ISO Image to the VM

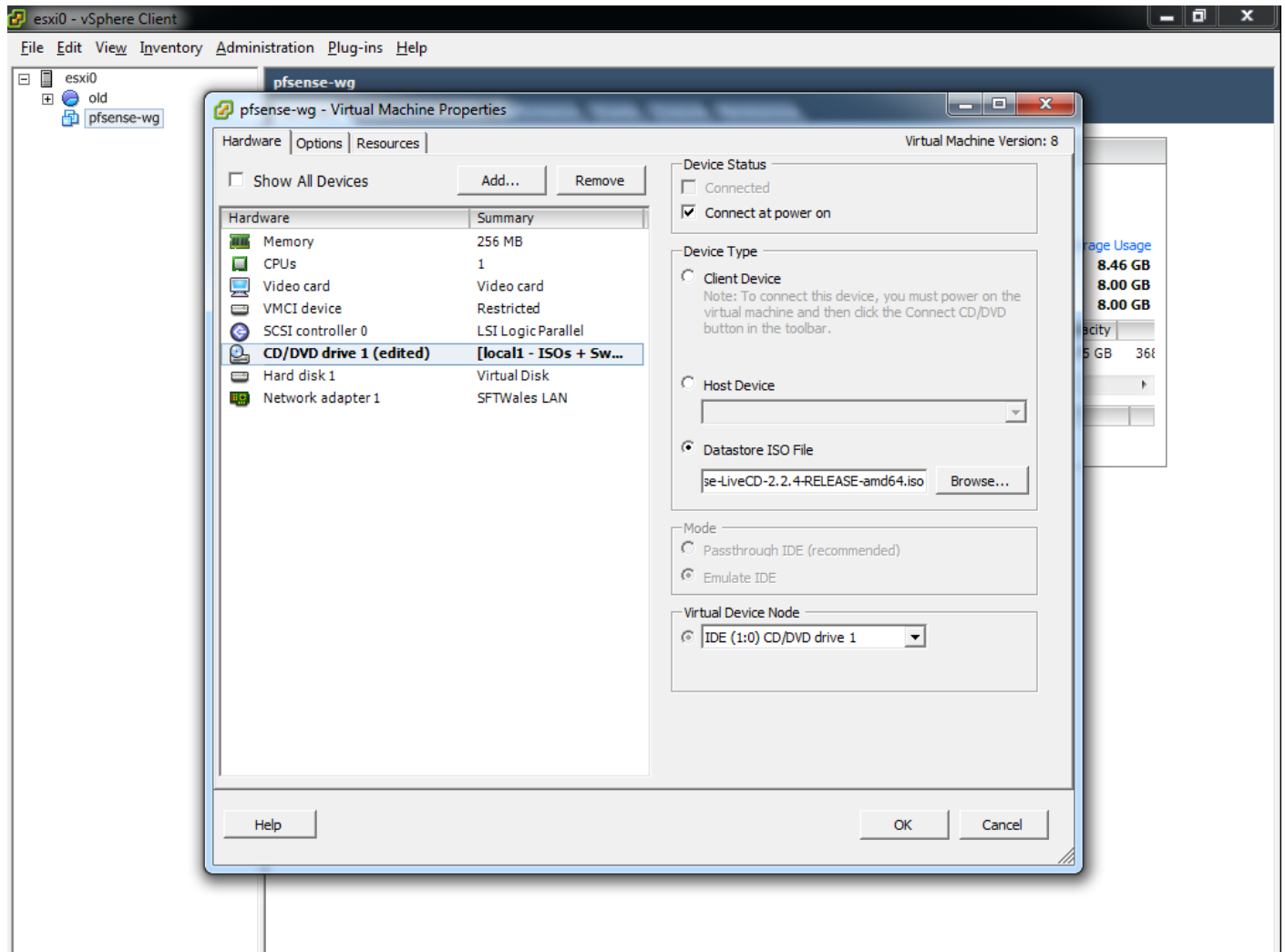
We now need to select the Virtual Machine ('pfsense-wg' in this case) and under Commands choose 'Edit Settings'



We now need to edit the CD/DVD Drive. Under device type choose 'Datastore ISO File' and Browse



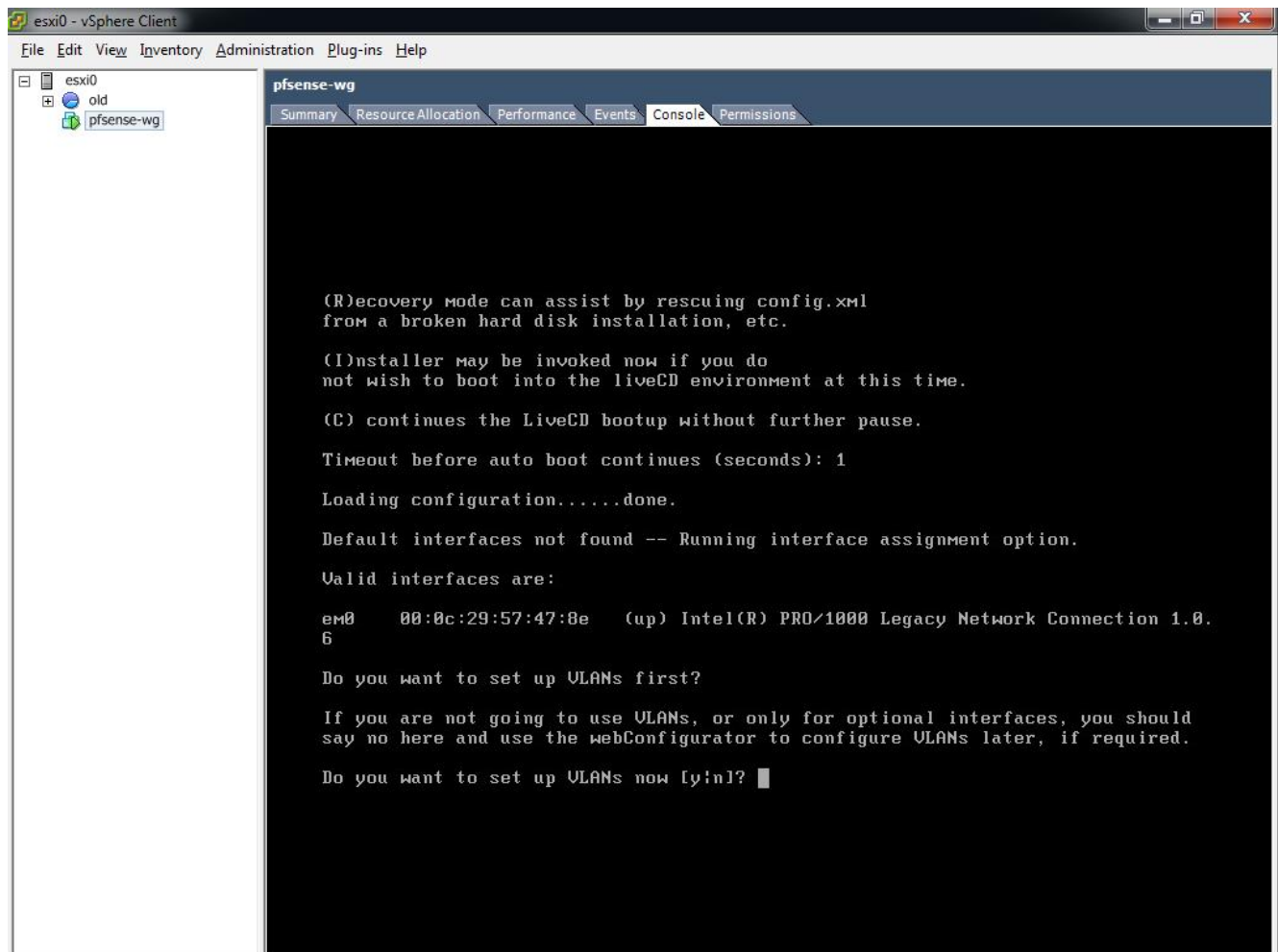
Ensure that the option for 'Connect at power on' is ticked



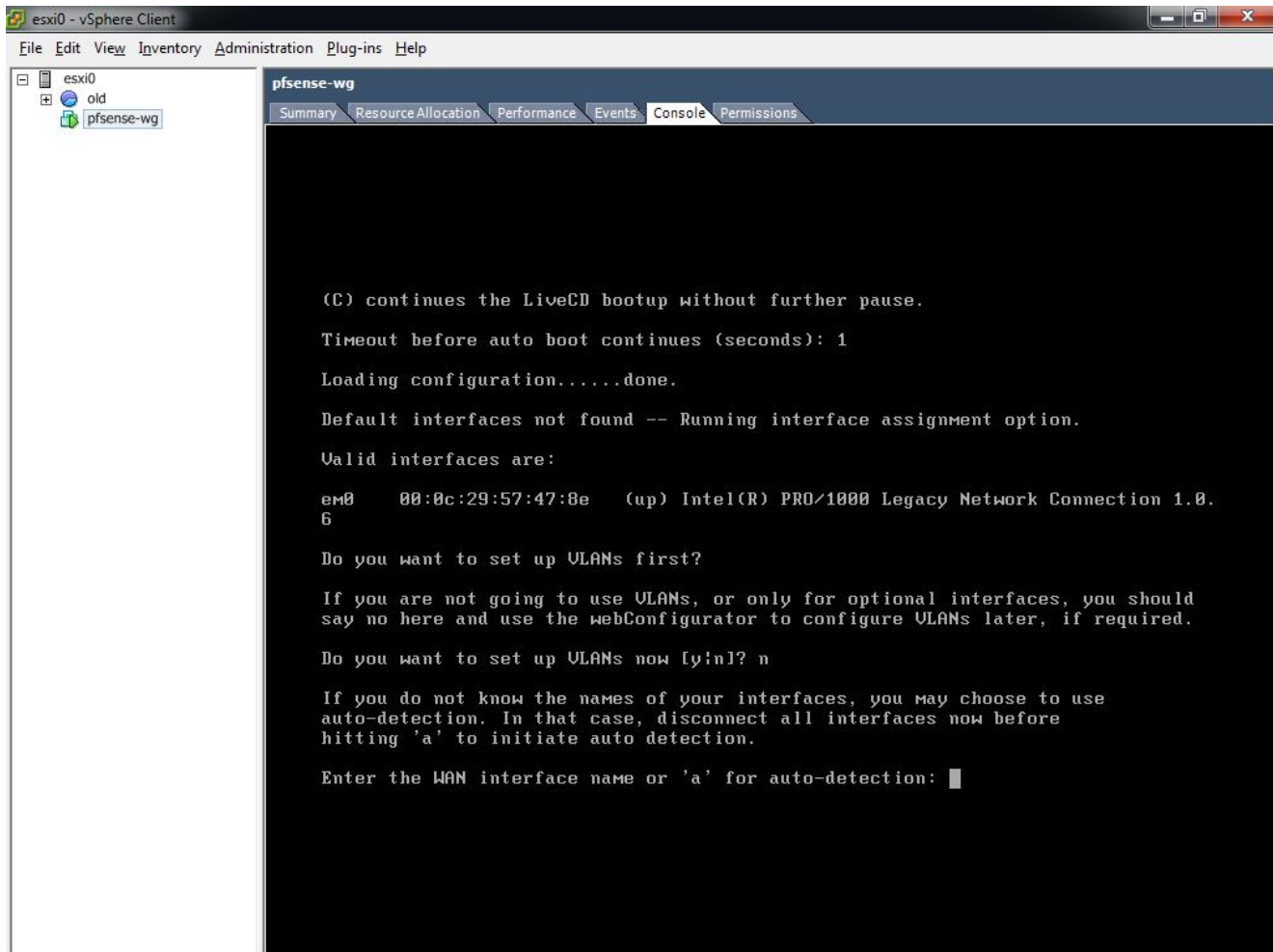


## pfSense Installation

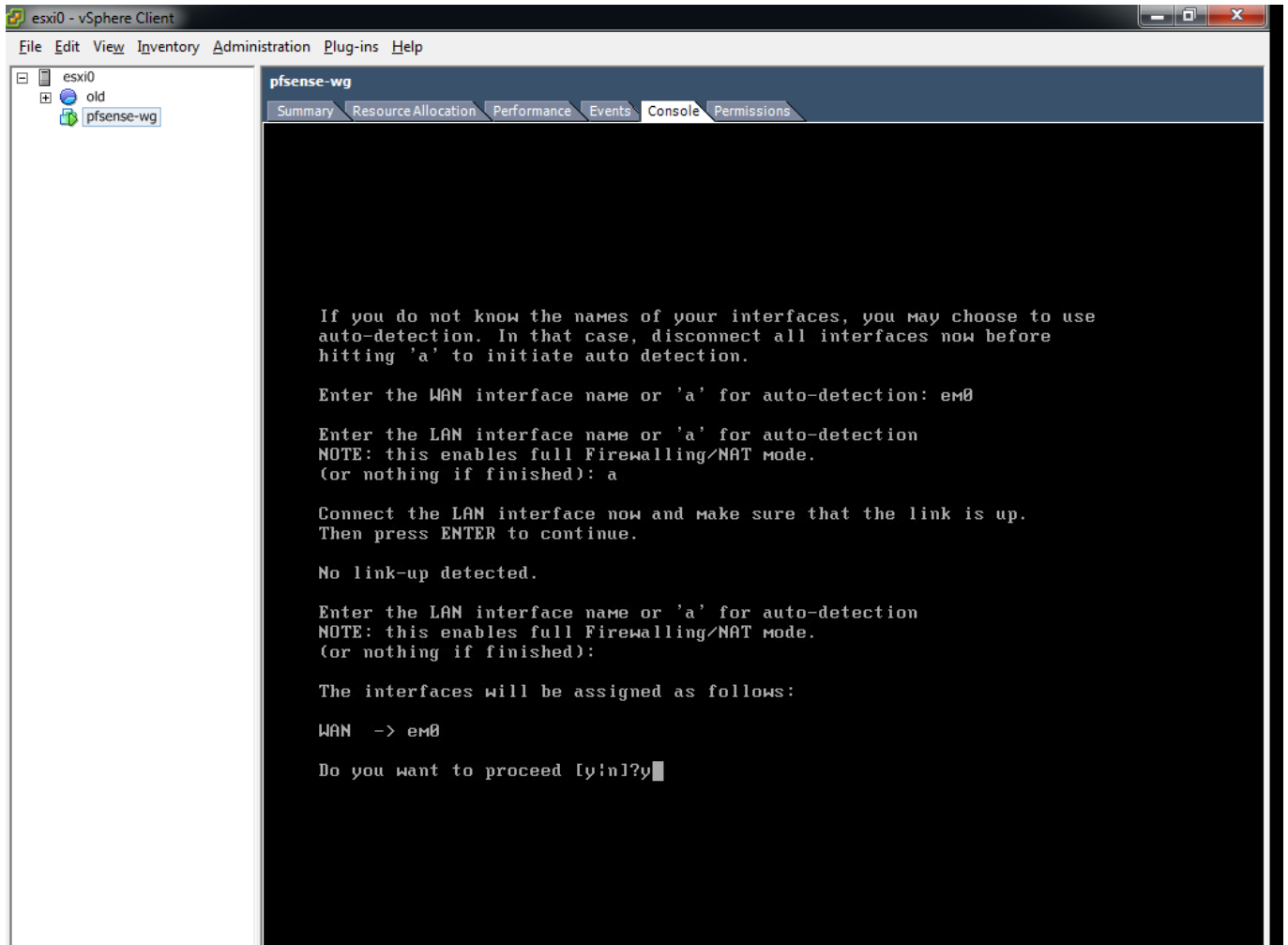
- Within a VM installation you are unlikely to want to setup VLANs, these can be handled within the Hypervisor i.e. VMWare, in this case choose 'n'
- Within a Physical server you may need to setup VLANs, In this case choose 'y'



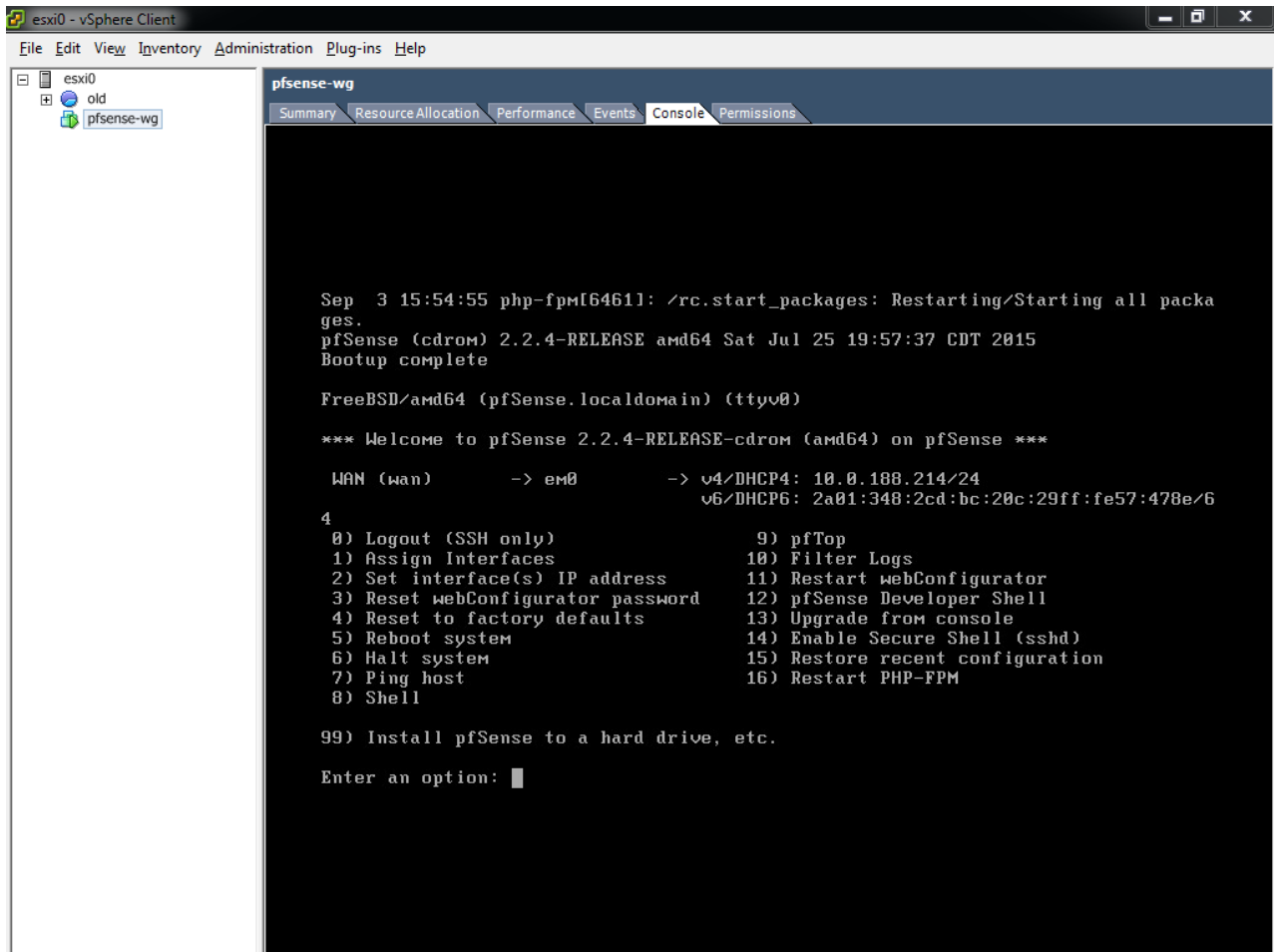
When prompted for the WAN interface enter the valid interface lists above i.e. 'emo'



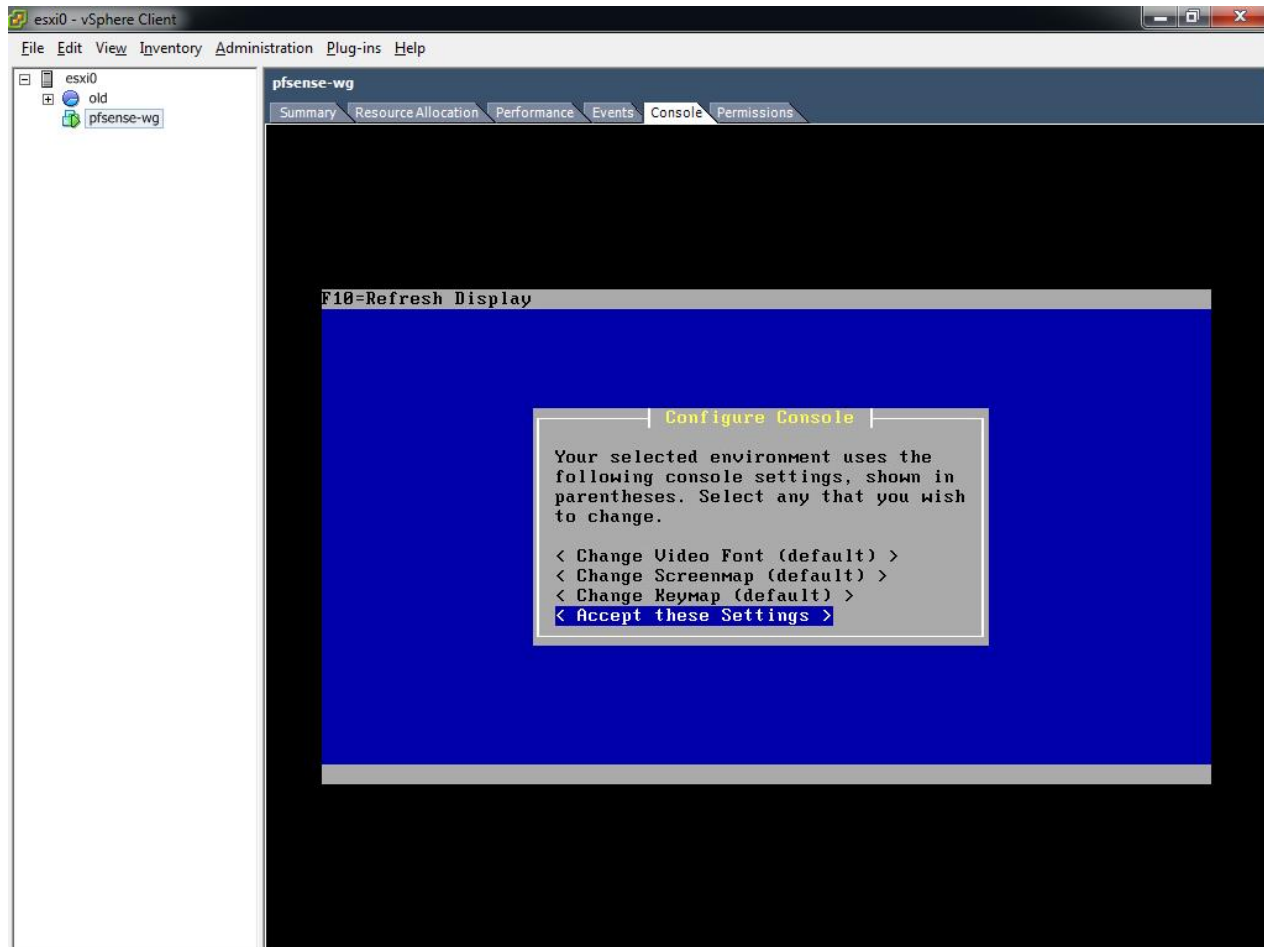
When prompted for a LAN interface choose 'a' for auto. Finally when it asks how 'interfaces will be assigned' check and choose 'y'



Next you will need to 'Install pfSense to a hard drive, etc..' enter '99'



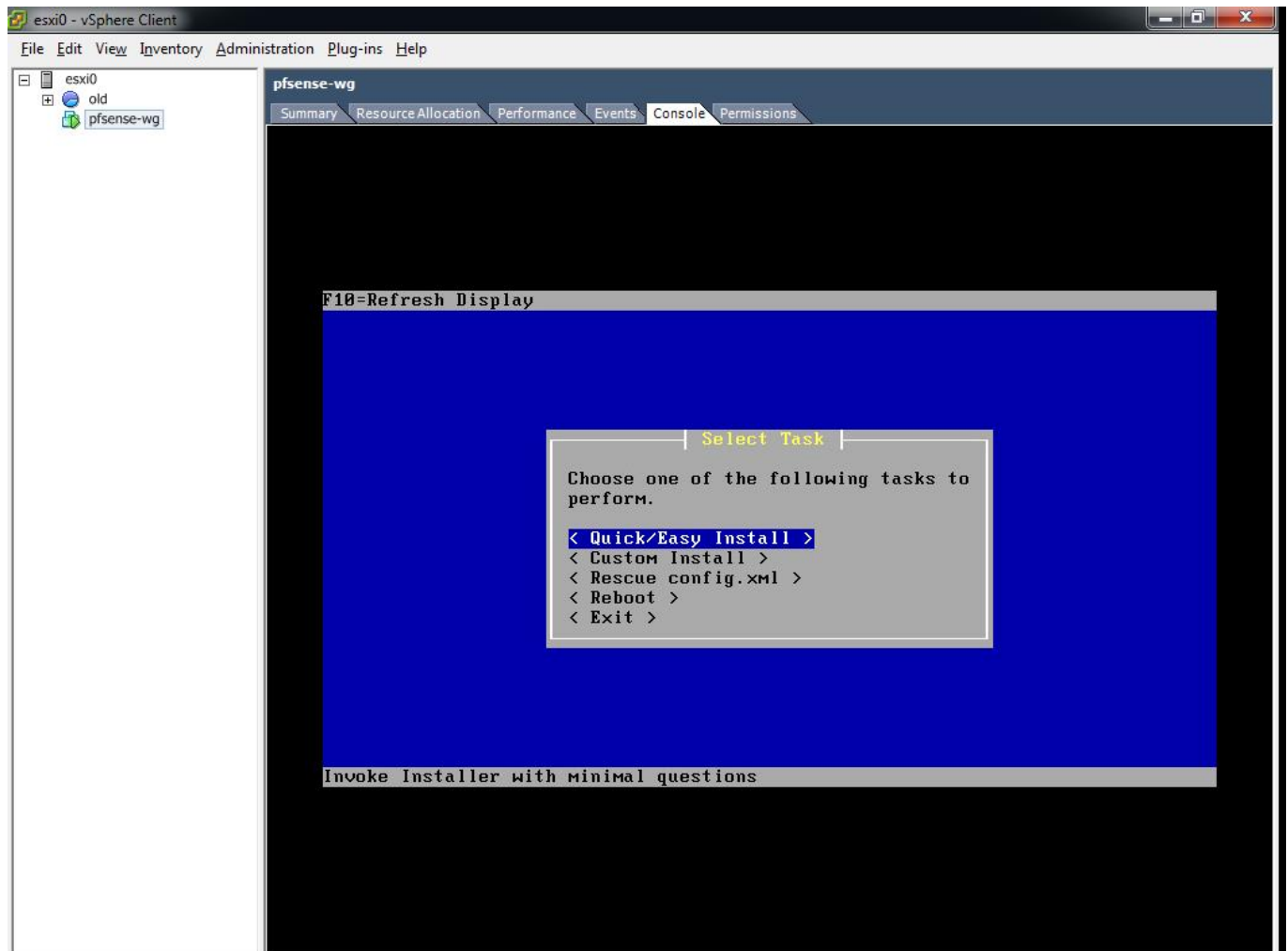
There is usually little reason to change options here. Choose 'Accept these Settings'



For a new installation on a VM, then choose Quick/Easy Install.

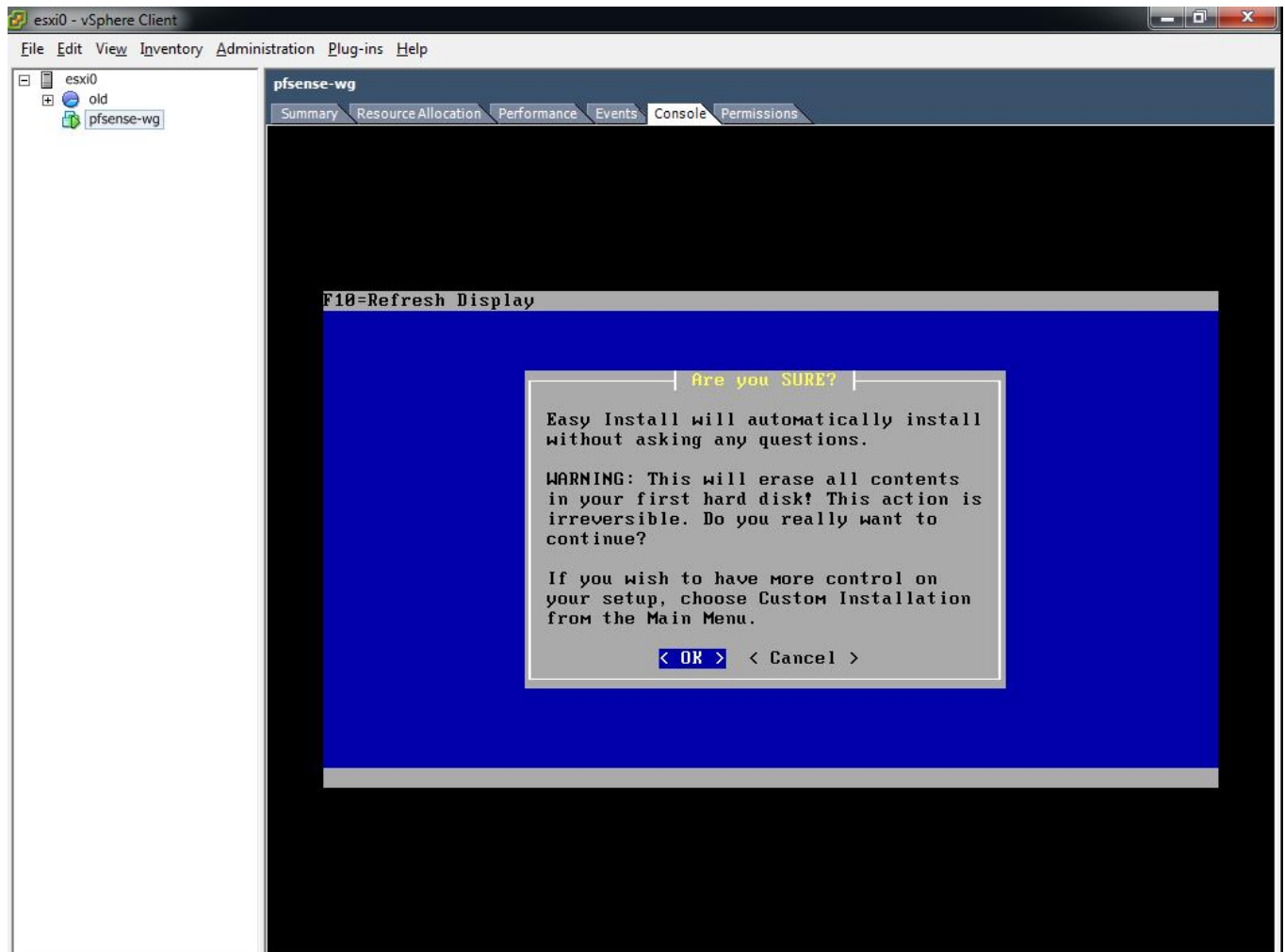
Custom Install can be used for features like 'Software RAID' (using two hard disks to provide RAID, but without a Hardware RAID controller)

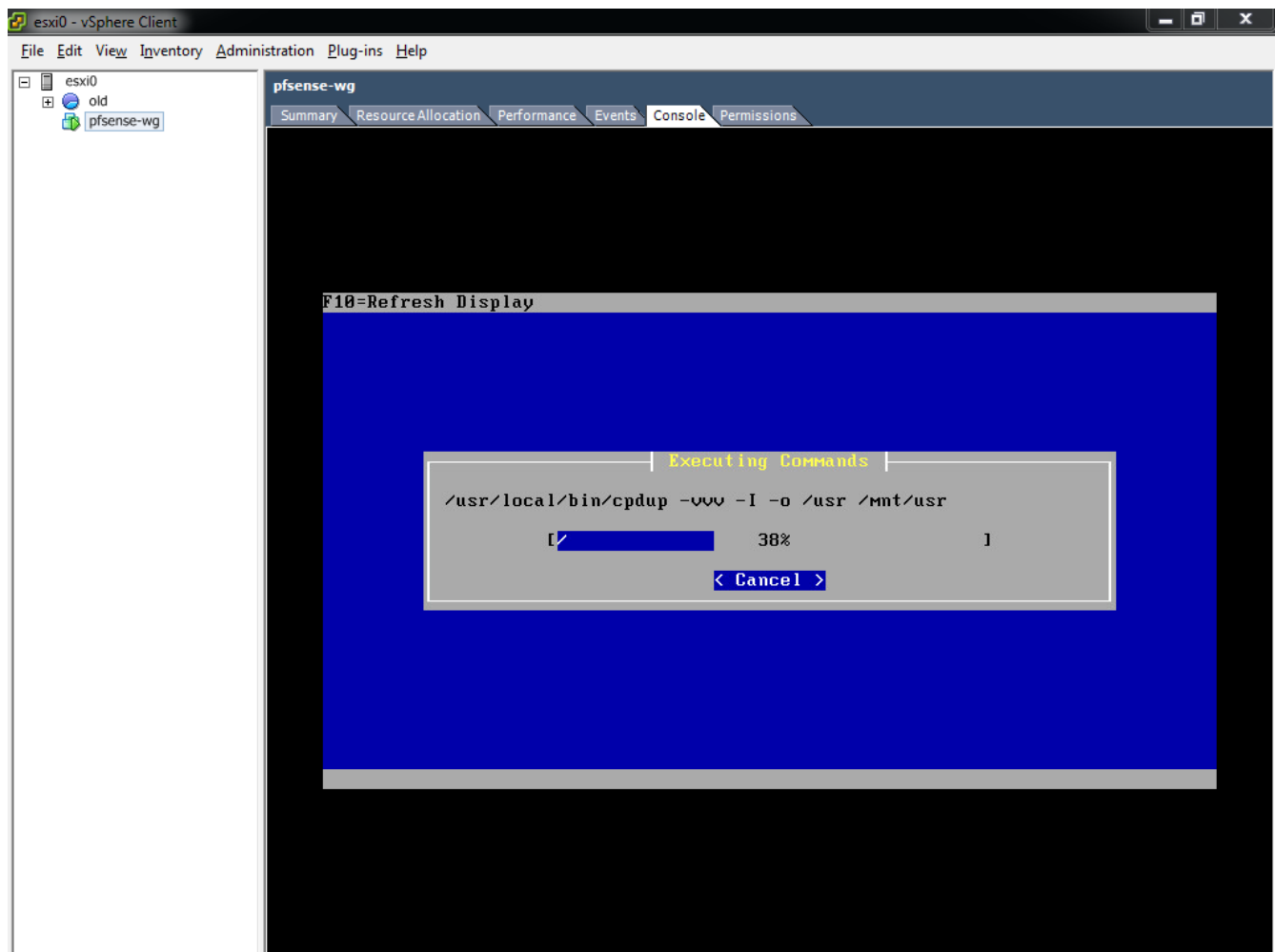
Rescue config.xml can be used to restore a backup, so for a re-installation.



For a new VM installation there should be nothing to consider here, just choose 'OK'

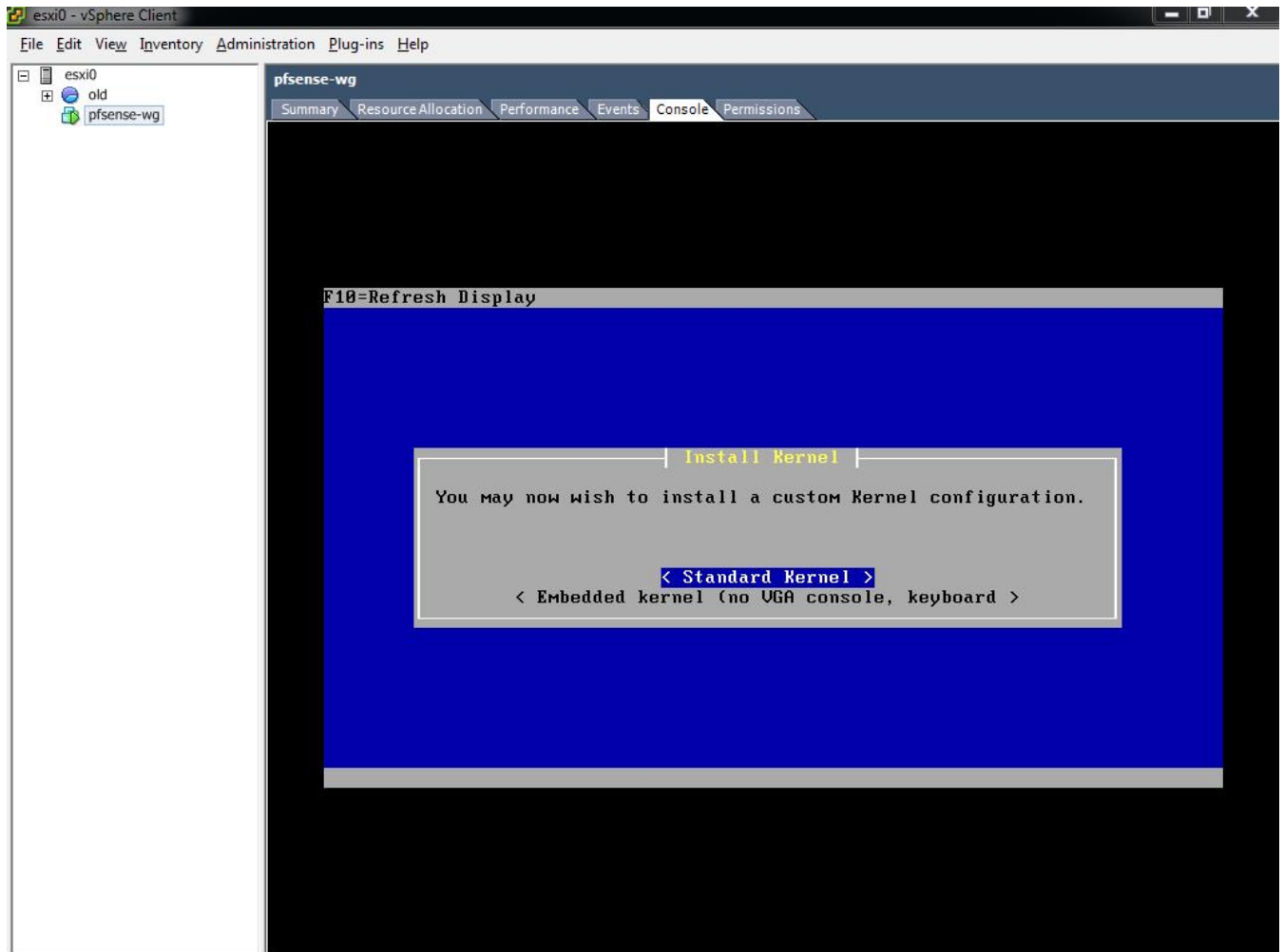
For any other installation take more notice, especially if you have any disks containing data you may wish to retain.



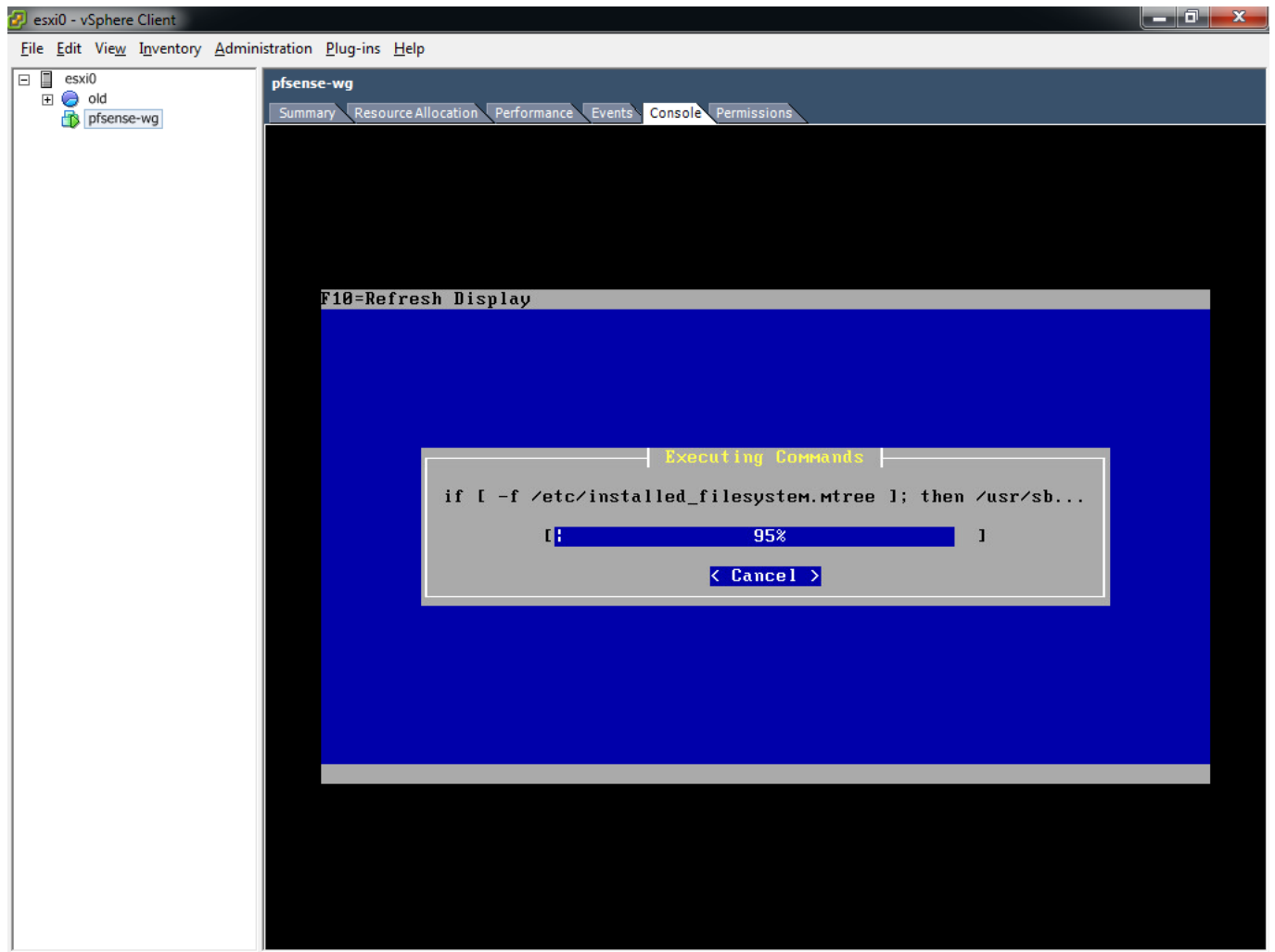




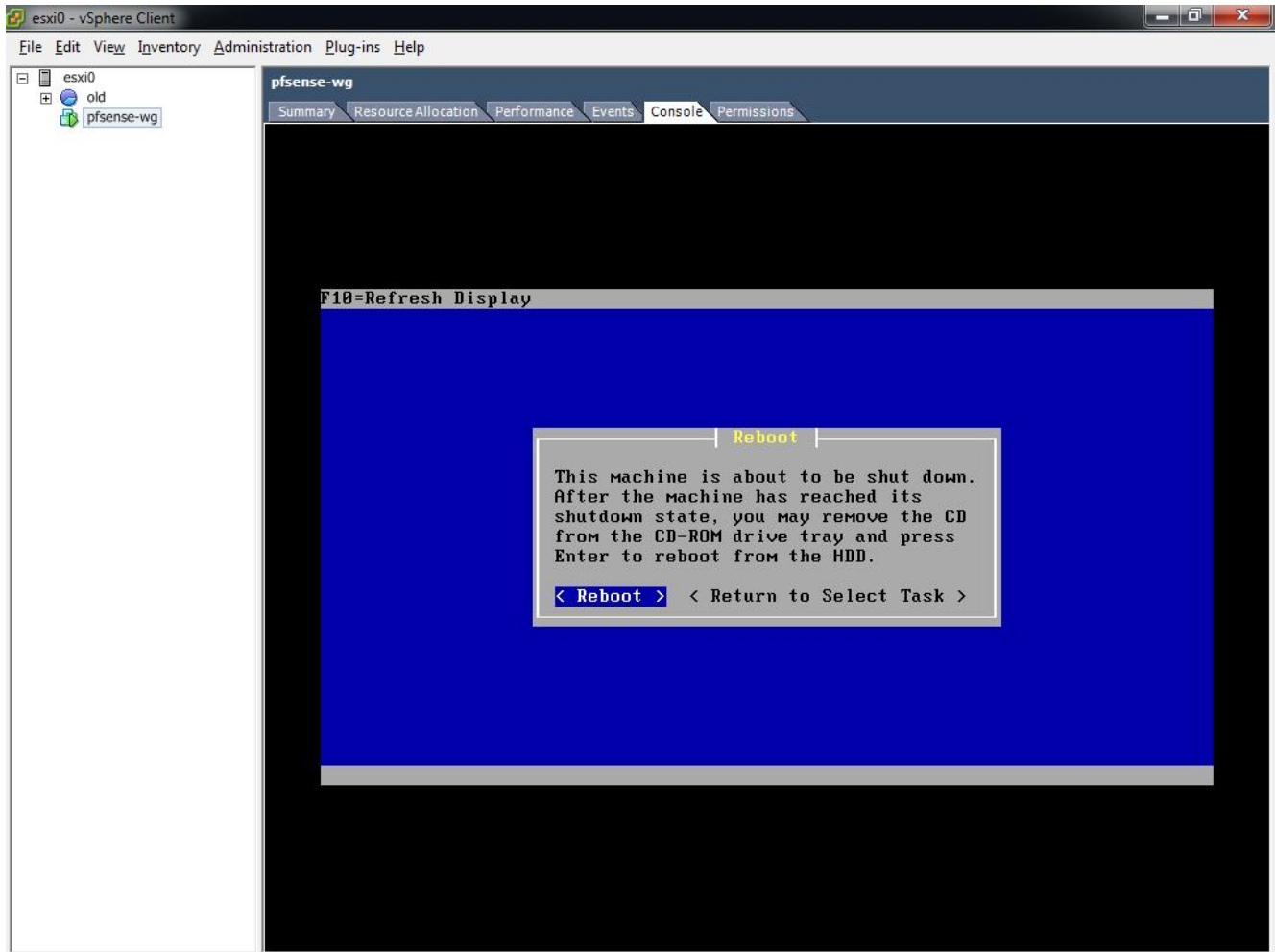
Once again for a VM installation we can go with the default, so choose 'Standard Kernel'. For some physical hardware installations you may want to use the 'Embedded kernel'



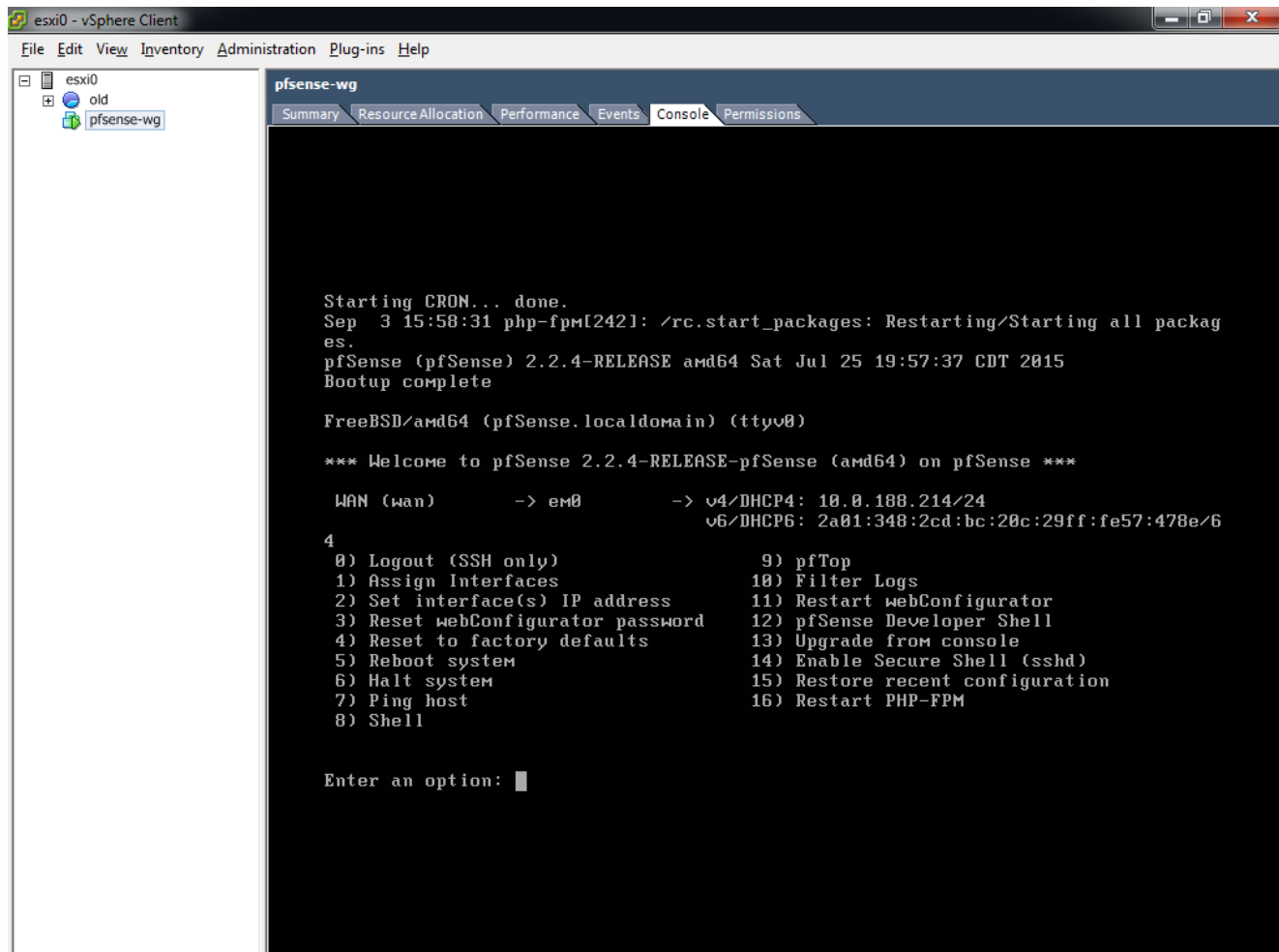
The installation will be copying files for a short time



Finally when the installation is complete, you can choose to 'reboot'



After a reboot, you should be presented with a screen similar to the following, showing that pfSense is now installed. Make a note of the WAN IP address, as you will need to visit this in a Web Browser.



The screenshot shows a vSphere Client window titled 'esxi0 - vSphere Client'. The left sidebar shows a tree view with 'esxi0' expanded, containing 'old' and 'pfsense-wg'. The main console window for 'pfsense-wg' has tabs for 'Summary', 'Resource Allocation', 'Performance', 'Events', 'Console', and 'Permissions'. The 'Console' tab is active, displaying the following text:

```
Starting CRON... done.
Sep  3 15:58:31 php-fpm[2421]: /rc.start_packages: Restarting/Starting all packages.
pfSense (pfSense) 2.2.4-RELEASE amd64 Sat Jul 25 19:57:37 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.188.214/24
                                v6/DHCP6: 2a01:348:2cd:bc:20c:29ff:fe57:478e/6

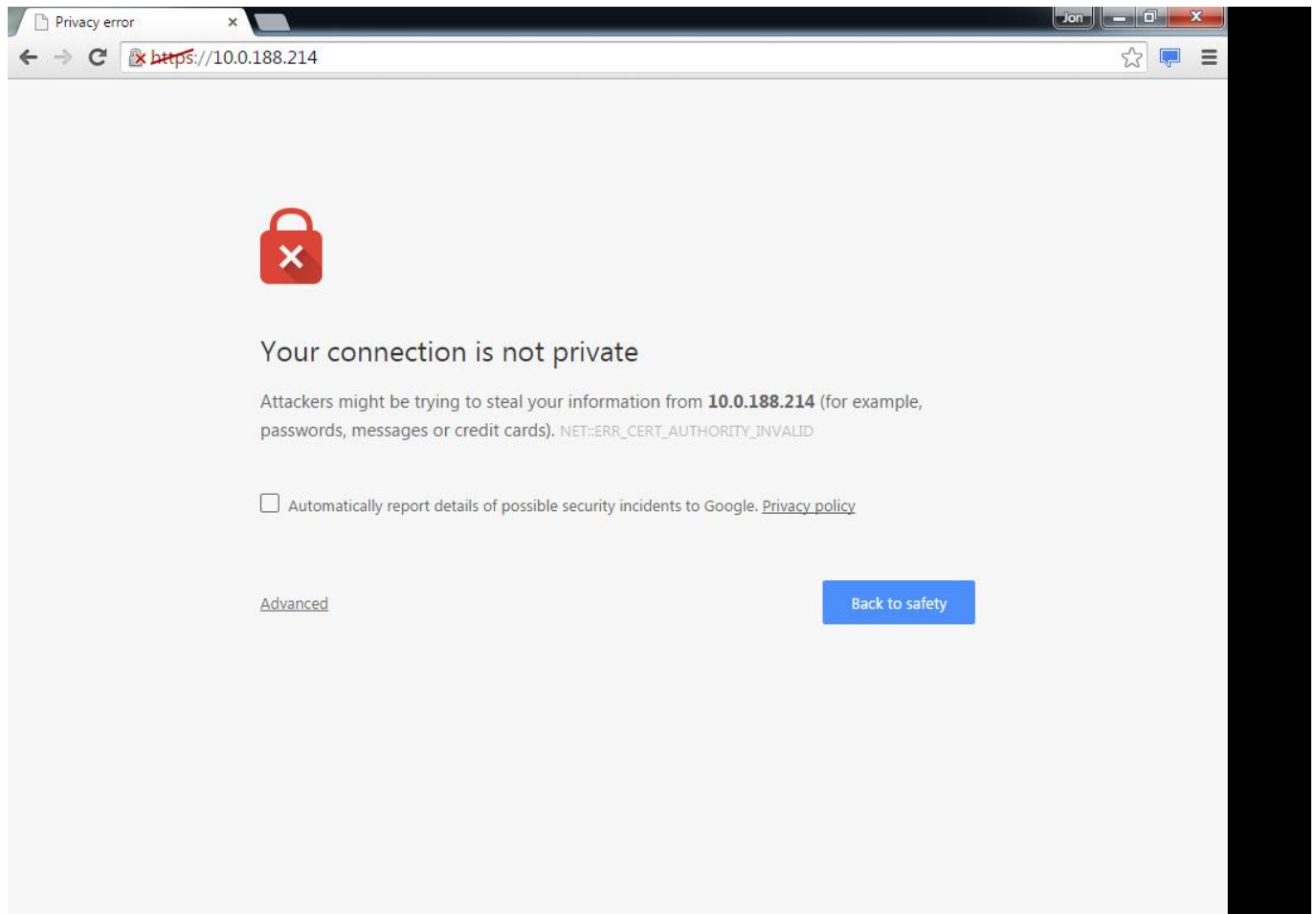
4
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

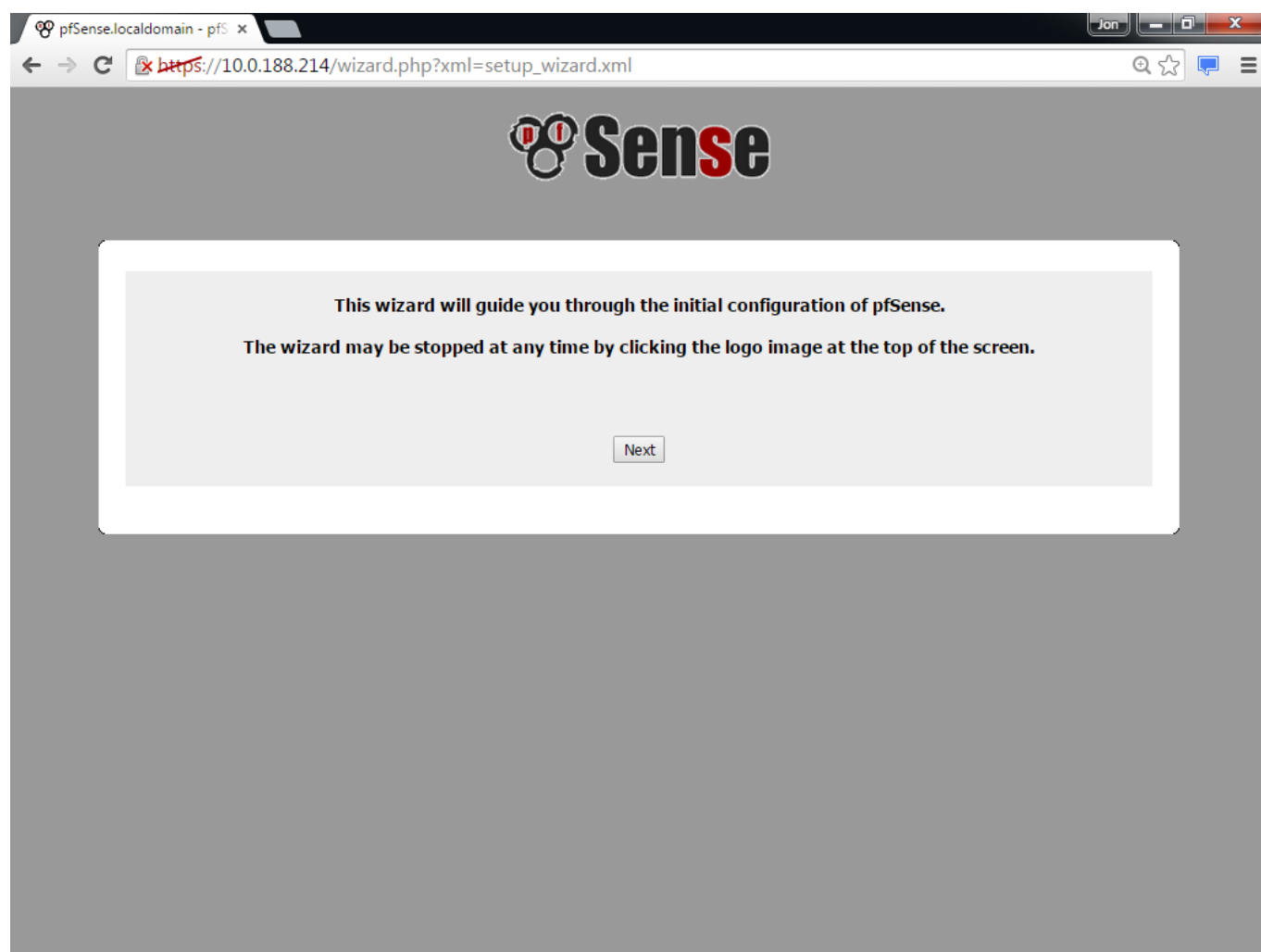
## Configuring pfSense

Visit the WAN IP address via https in your Web Browser in the example <https://10.0.188.214>.

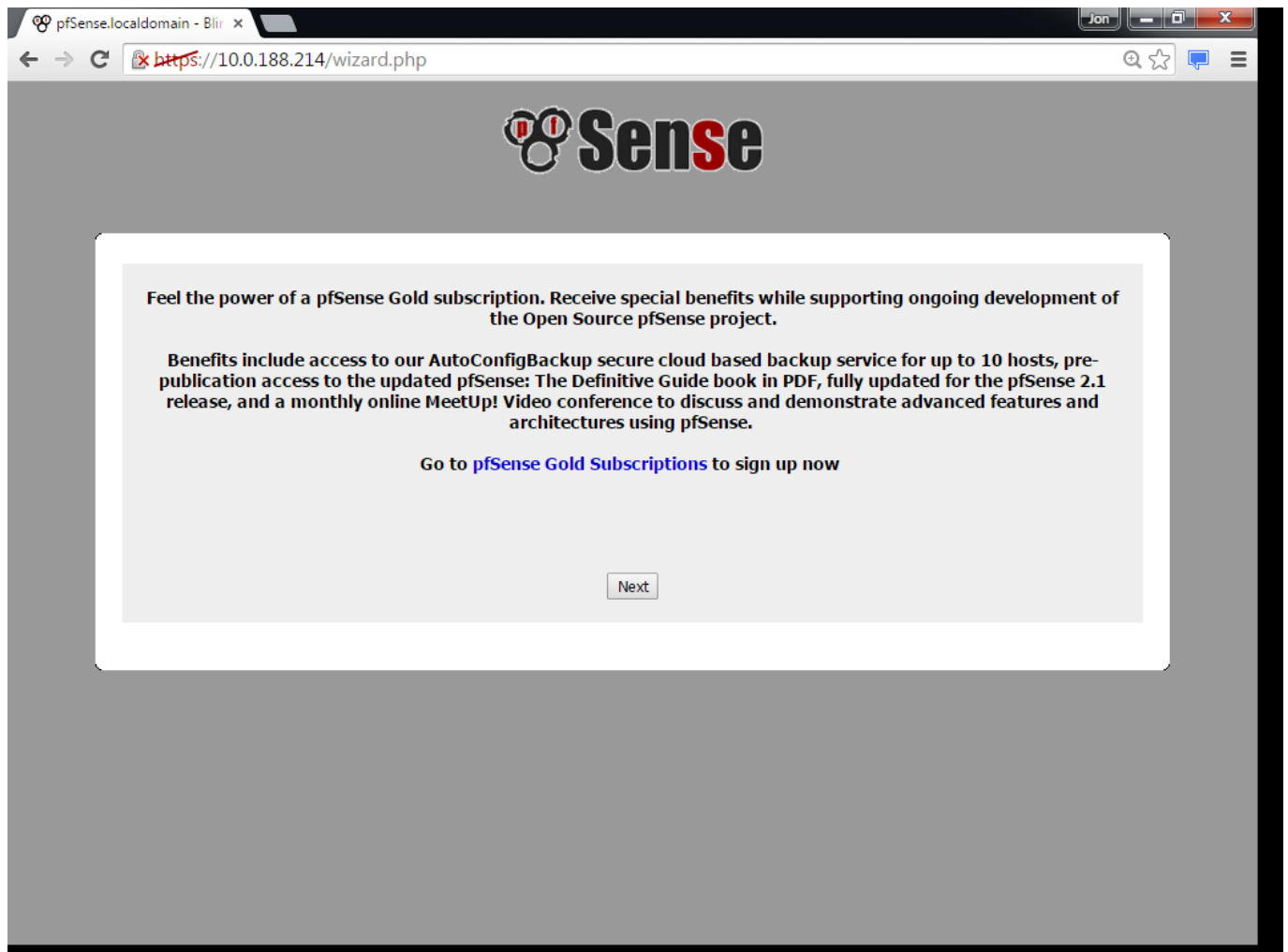
You will need to accept the Self-Signed certificate that is used within pfSense



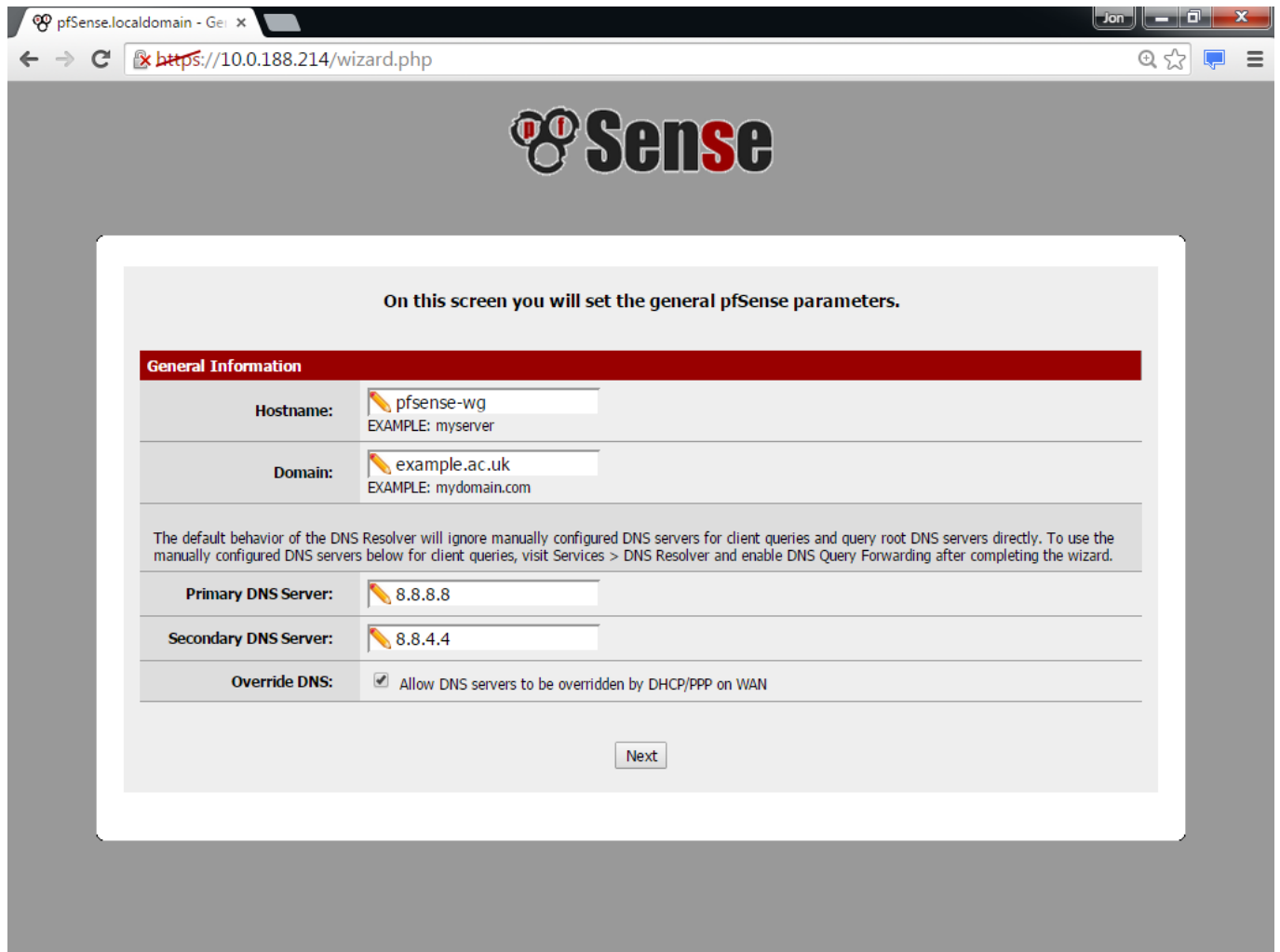
On the initial screen click 'Next'



The following screen advertises the Commercial support available via a pfSense gold subscription.



On this screen we provide the hostname and domain



The screenshot shows a web browser window with the URL `https://10.0.188.214/wizard.php`. The page features the pfSense logo at the top. Below the logo, a message states: "On this screen you will set the general pfSense parameters." The main content area is titled "General Information" and contains several input fields and a checkbox. The "Hostname" field is set to "pfsense-wg" with an example of "myserver". The "Domain" field is set to "example.ac.uk" with an example of "mydomain.com". Below these fields, a note explains the default behavior of the DNS Resolver. The "Primary DNS Server" field is set to "8.8.8.8" and the "Secondary DNS Server" field is set to "8.8.4.4". The "Override DNS" checkbox is checked, with the label "Allow DNS servers to be overridden by DHCP/PPP on WAN". A "Next" button is located at the bottom right of the form.

On this screen you will set the general pfSense parameters.

**General Information**

Hostname:   
EXAMPLE: myserver

Domain:   
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

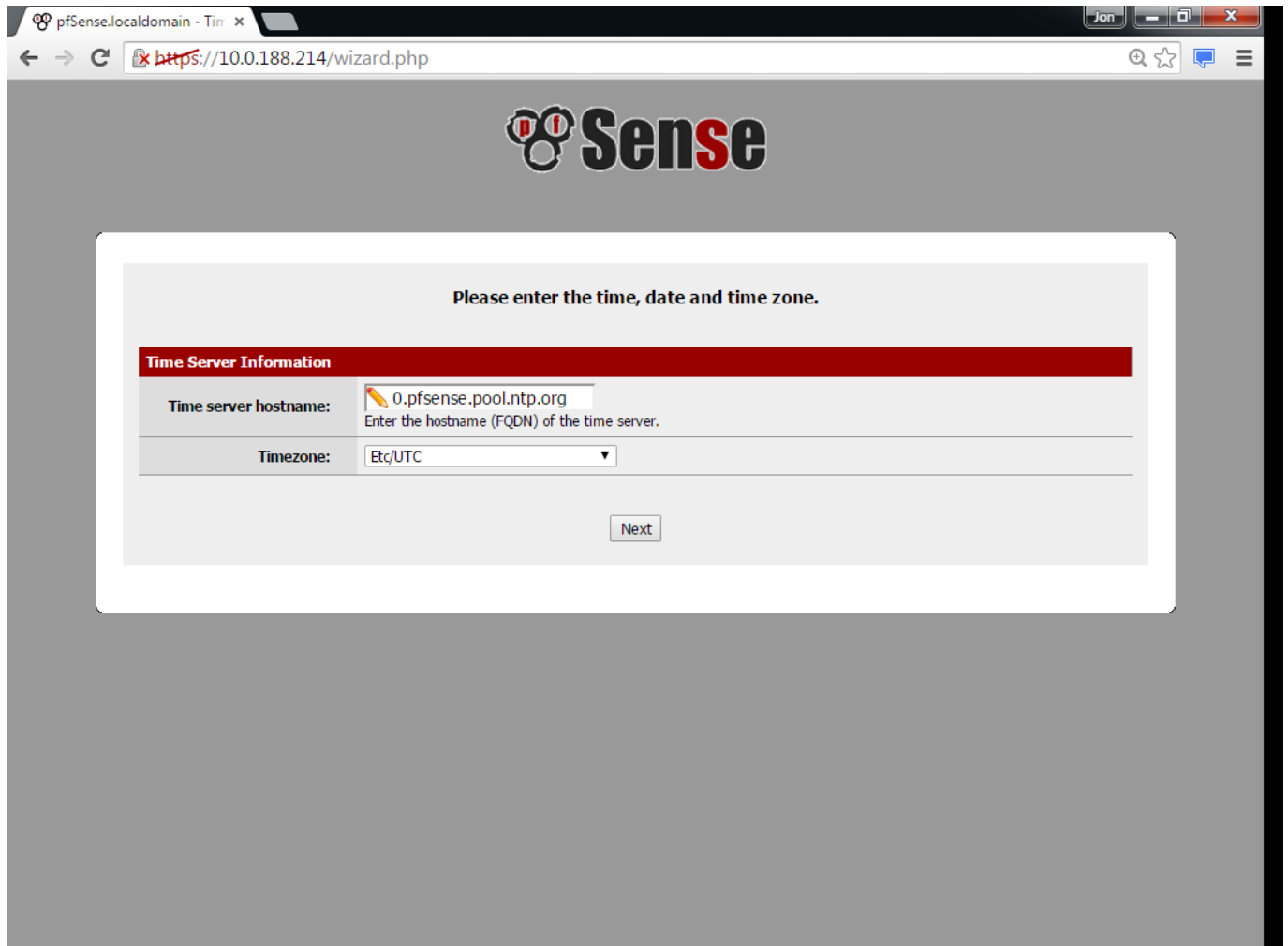
Secondary DNS Server:

Override DNS: ☒ Allow DNS servers to be overridden by DHCP/PPP on WAN

Next



Here you may provide any Time zone and NTP server settings. If you have a local NTP server enter it here.



The screenshot shows a web browser window with the address bar displaying `https://10.0.188.214/wizard.php`. The page features the pfSense logo at the top. Below the logo, a white box contains the instruction "Please enter the time, date and time zone." Underneath this, a red header bar reads "Time Server Information". The form includes two fields: "Time server hostname:" with a text input containing `0.pfsense.pool.ntp.org` and a subtext "Enter the hostname (FQDN) of the time server.", and "Timezone:" with a dropdown menu currently set to "Etc/UTC". A "Next" button is positioned at the bottom right of the form.

Time Server Information	
Time server hostname:	<input type="text" value="0.pfsense.pool.ntp.org"/> <small>Enter the hostname (FQDN) of the time server.</small>
Timezone:	<input type="text" value="Etc/UTC"/>

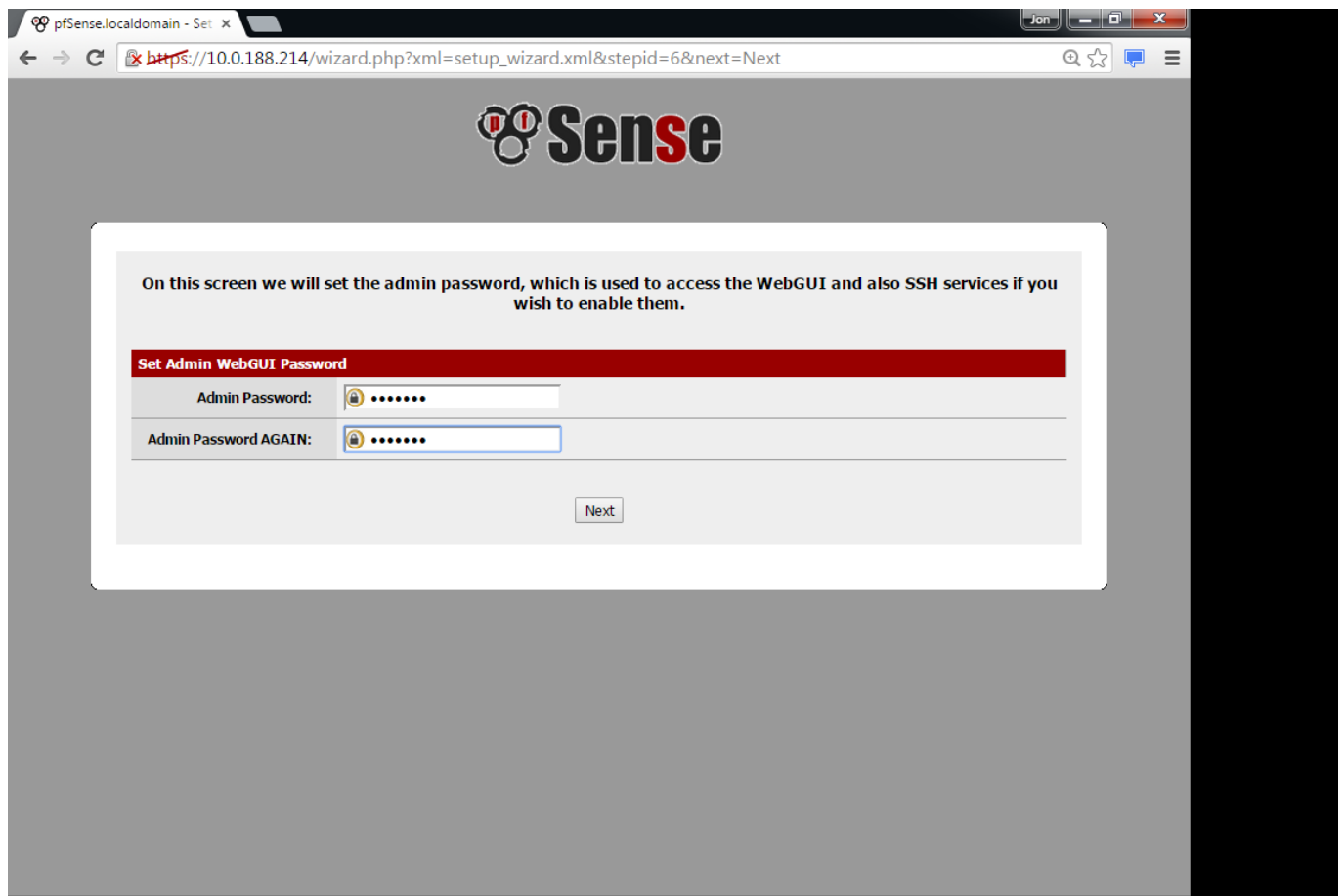
Next

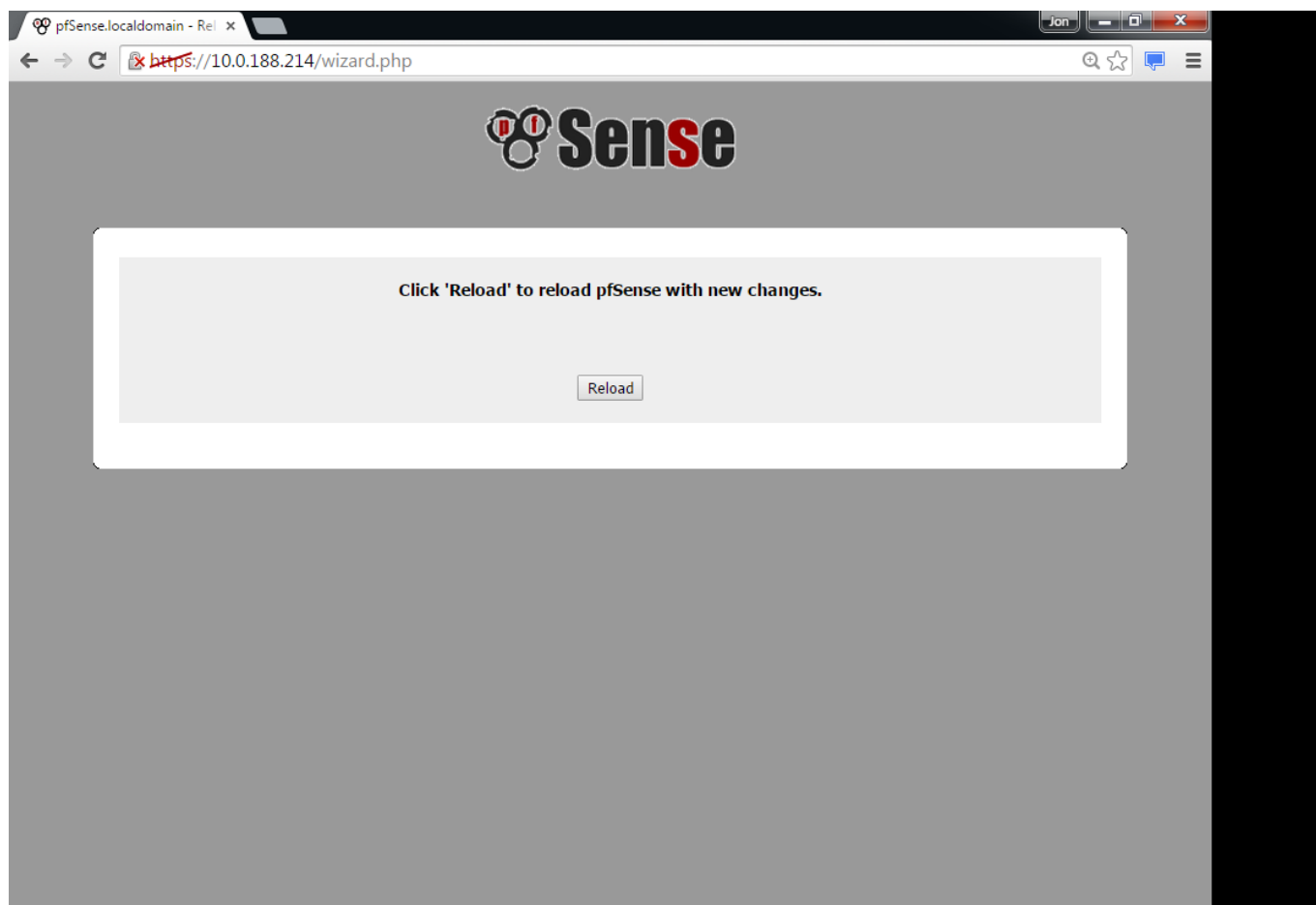
On this screen you may wish to remove the tick related to 'Block RFC1918 Private Networks', especially if the WAN interface is on such a network.

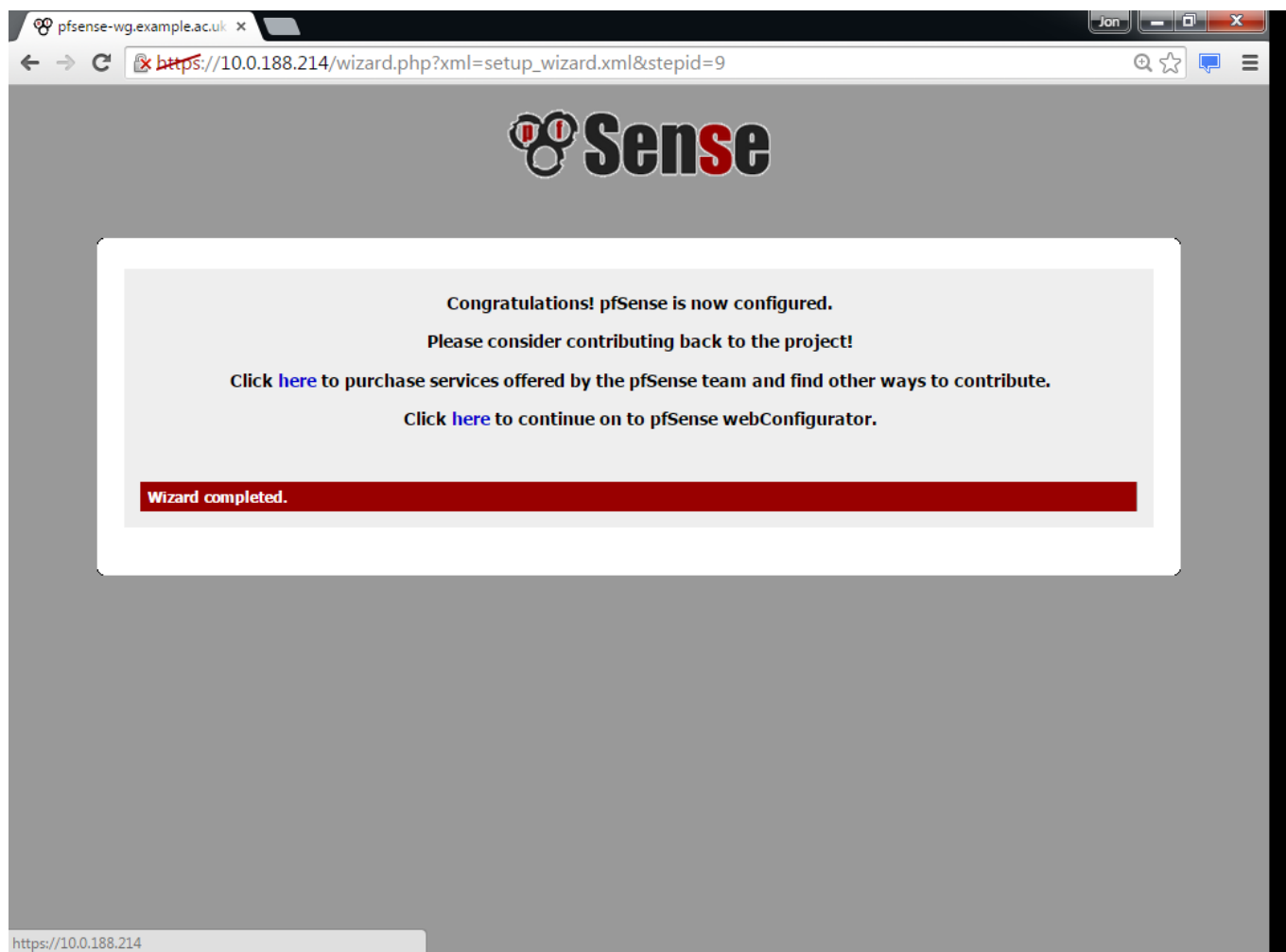
The screenshot shows the pfSense configuration wizard at the URL `https://10.0.188.214/wizard.php`. The page is titled "pfSense.localdomain - Config" and contains the following sections:

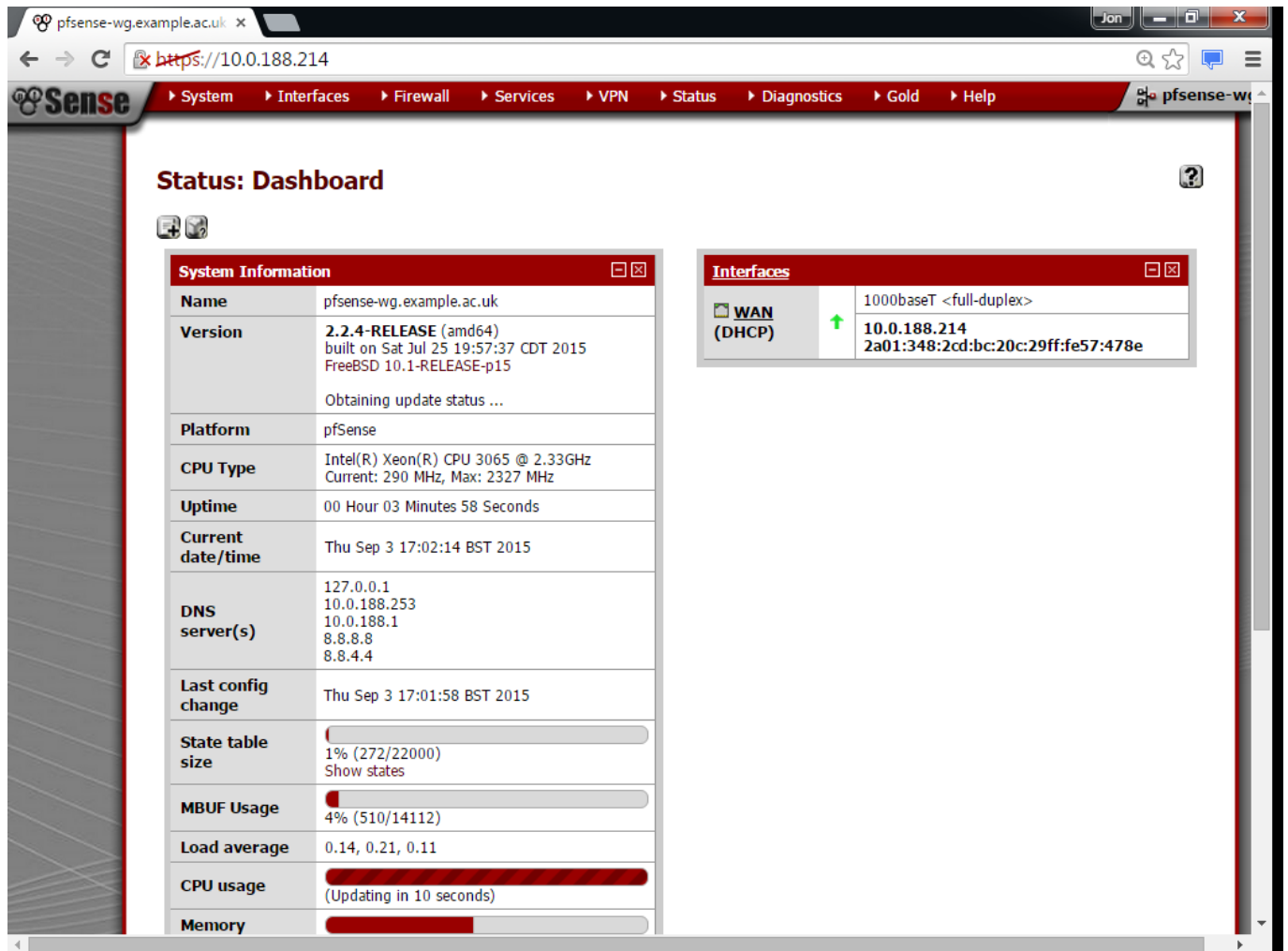
- PPPoE Idle timeout:** A text input field with a pencil icon. Description: "If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature."
- PPTP configuration** (Section Header):
  - PPTP Username:** A text input field with a pencil icon.
  - PPTP Password:** A text input field with a pencil icon.
  - PPTP Local IP Address:** A text input field with a pencil icon, followed by a dropdown menu showing "1".
  - PPTP Remote IP Address:** A text input field with a pencil icon.
  - PPTP Dial on demand:** A checkbox. Description: "This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. Enable Dial-On-Demand mode".
  - PPTP Idle timeout:** A text input field with a pencil icon. Description: "If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature."
- RFC1918 Networks** (Section Header):
  - Block RFC1918 Private Networks:** A checkbox. Description: "When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too. Block private networks from entering via WAN".
- Block bogon networks** (Section Header):
  - Block bogon networks:** A checkbox. Description: "When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive. Block non-Internet routed networks from entering via WAN".

A "Next" button is located at the bottom of the form.









The screenshot shows the pfSense web interface in a browser window. The address bar displays `https://10.0.188.214`. The navigation menu at the top includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Status: Dashboard" and contains two panels: "System Information" and "Interfaces".

**System Information**

Name	pfSense-wg.example.ac.uk
Version	2.2.4-RELEASE (amd64) built on Sat Jul 25 19:57:37 CDT 2015 FreeBSD 10.1-RELEASE-p15 Obtaining update status ...
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU 3065 @ 2.33GHz Current: 290 MHz, Max: 2327 MHz
Uptime	00 Hour 03 Minutes 58 Seconds
Current date/time	Thu Sep 3 17:02:14 BST 2015
DNS server(s)	127.0.0.1 10.0.188.253 10.0.188.1 8.8.8.8 8.8.4.4
Last config change	Thu Sep 3 17:01:58 BST 2015
State table size	1% (272/22000) Show states
MBUF Usage	4% (510/14112)
Load average	0.14, 0.21, 0.11
CPU usage	(Updating in 10 seconds)
Memory	

**Interfaces**

WAN (DHCP)	1000baseT <full-duplex> 10.0.188.214 2a01:348:2cd:bc:20c:29ff:fe57:478e
------------	---

## Adding a LAN Interface

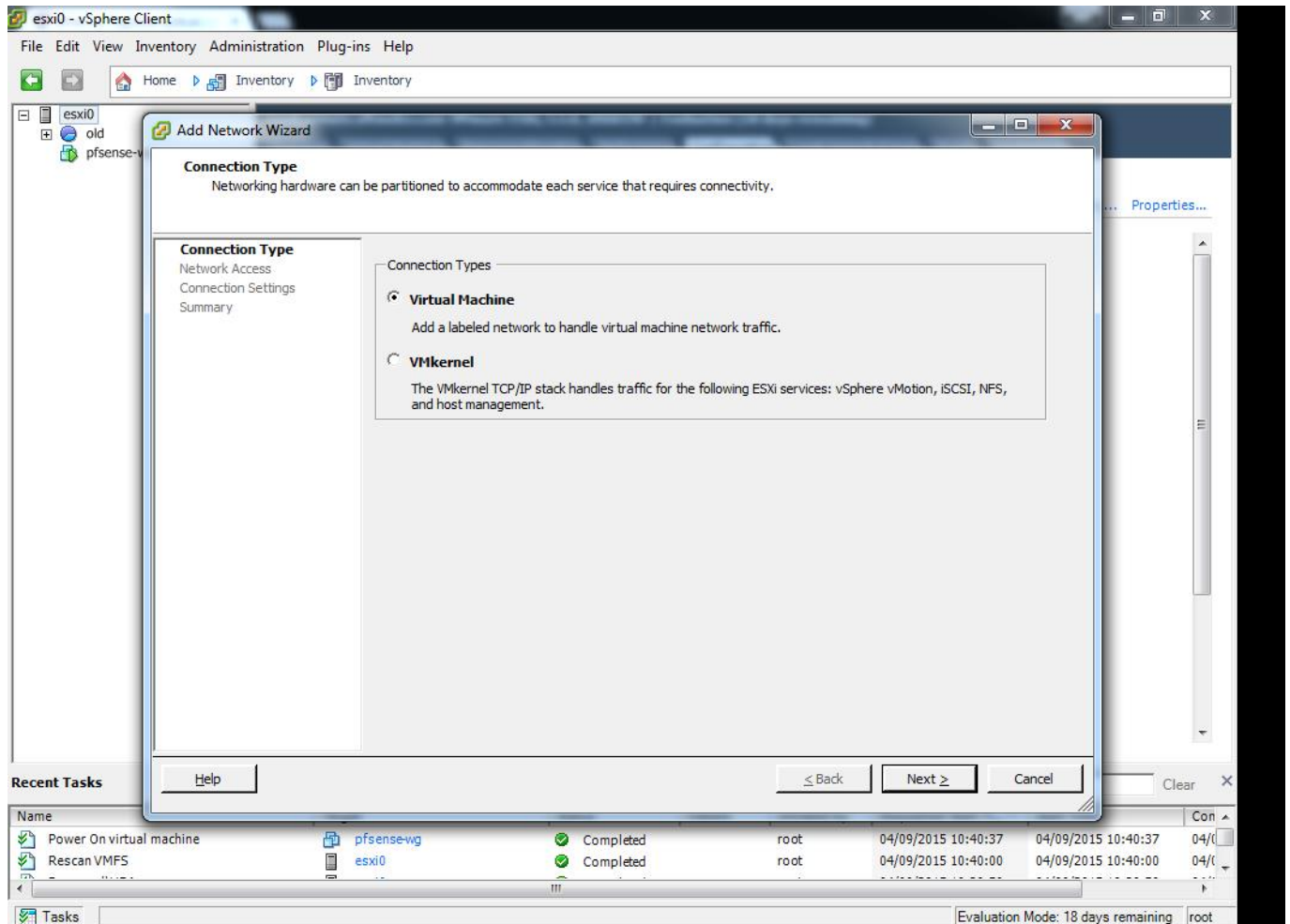
### VMWare ESXi Networking Configuration

Firstly confirm that you have the required LAN or VLAN configured as a Virtual Machine Port Group in VMWare. If you do then you can skip to the section on 'Virtual Machine Networking Configuration'. If you are using a Virtual Machine cluster then you should ensure that all Virtual Machine hosts (Hypervisors) are configured identically, or at least consistently.

The screenshot displays the VMware vSphere Client interface for an ESXi host. The 'View' tab is selected, showing the 'vSphere Standard Switch' configuration. The 'Networking' section is expanded, showing a list of Virtual Machine Port Groups connected to the vSwitch. The 'Recent Tasks' pane at the bottom shows a list of tasks, including 'Power On virtual machine' and 'Rescan VMFS', both completed.

Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completion Time
Power On virtual machine	pfSense-wg	Completed		root	04/09/2015 10:40:37	04/09/2015 10:40:37	04/09/2015 10:40:37
Rescan VMFS	esxi0	Completed		root	04/09/2015 10:40:00	04/09/2015 10:40:00	04/09/2015 10:40:00

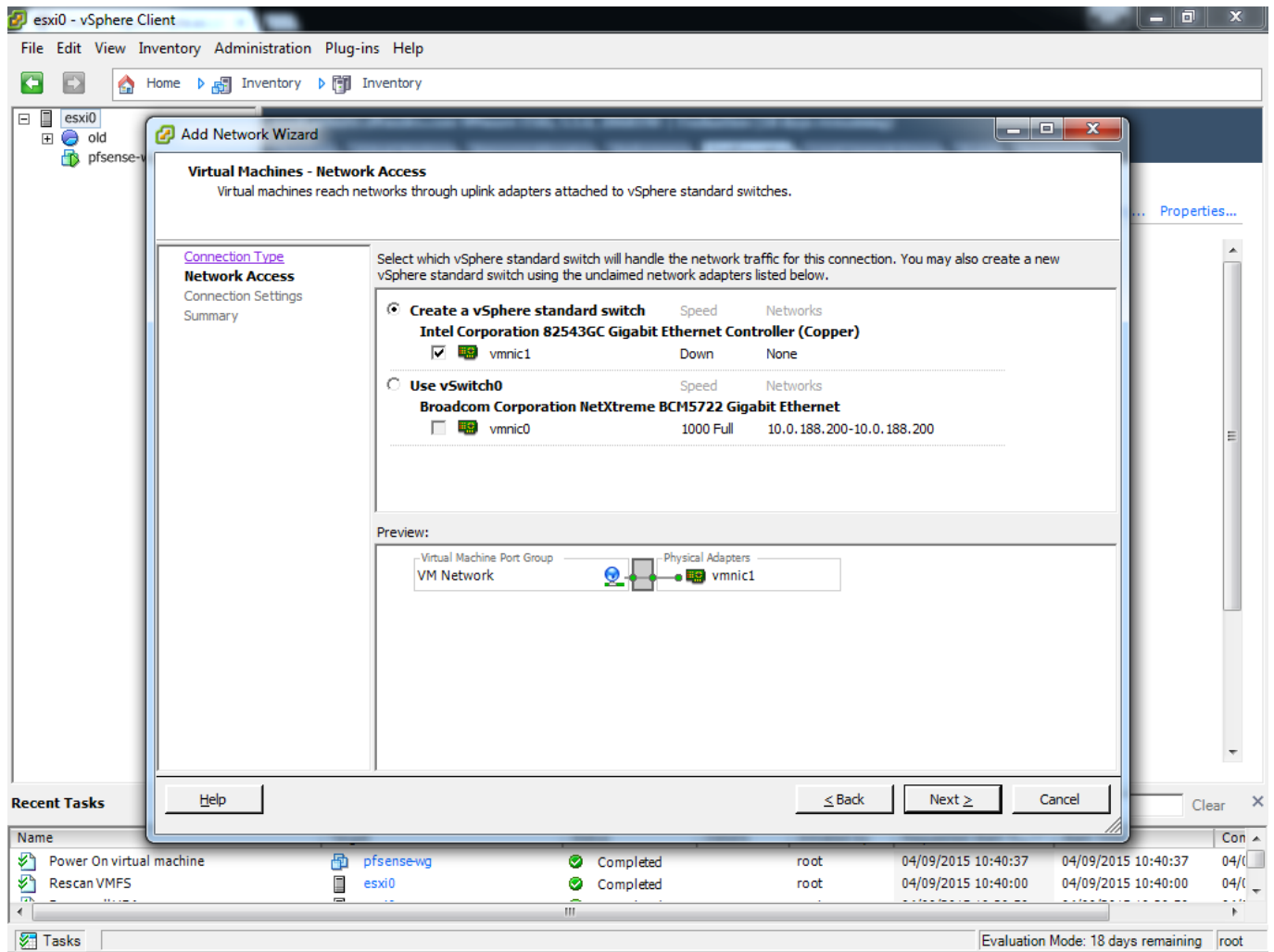
## Choose Add, and Virtual Machine



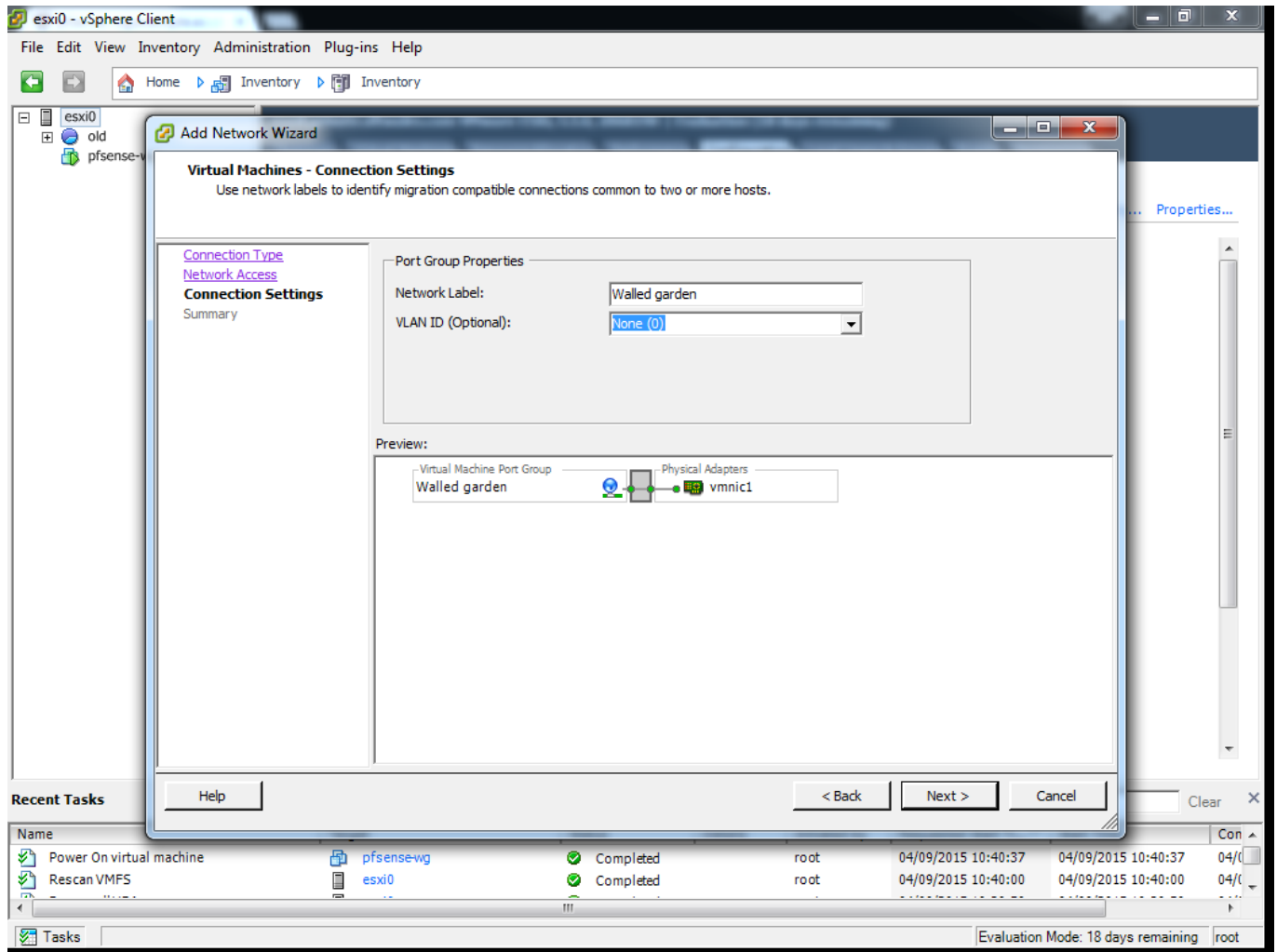
This screen is where you select the vmnic or vSwitch concerned.

- In this scenario we are using physical NIC on the ESXi server, this plugged directly into the wireless AP/Controller. You may see this in a production environment, where you are using a physical NIC to the VMWare server and untagged/access VLAN on the corresponding switch
- In most production environments you will be making use of existing NICs, and therefore an existing vSwitch and select the correct VLAN ID.





On this screen we give the network a label. It's important that label is consistent across a Virtual Machine cluster. The VLAN ID, in this case (and in cases where the port from the physical network switch into VMWare is configured as an untagged/access VLAN) then you leave it as 'None (0)'. For instances with a tagged/trunk VLAN port you would enter the VLAN ID here.



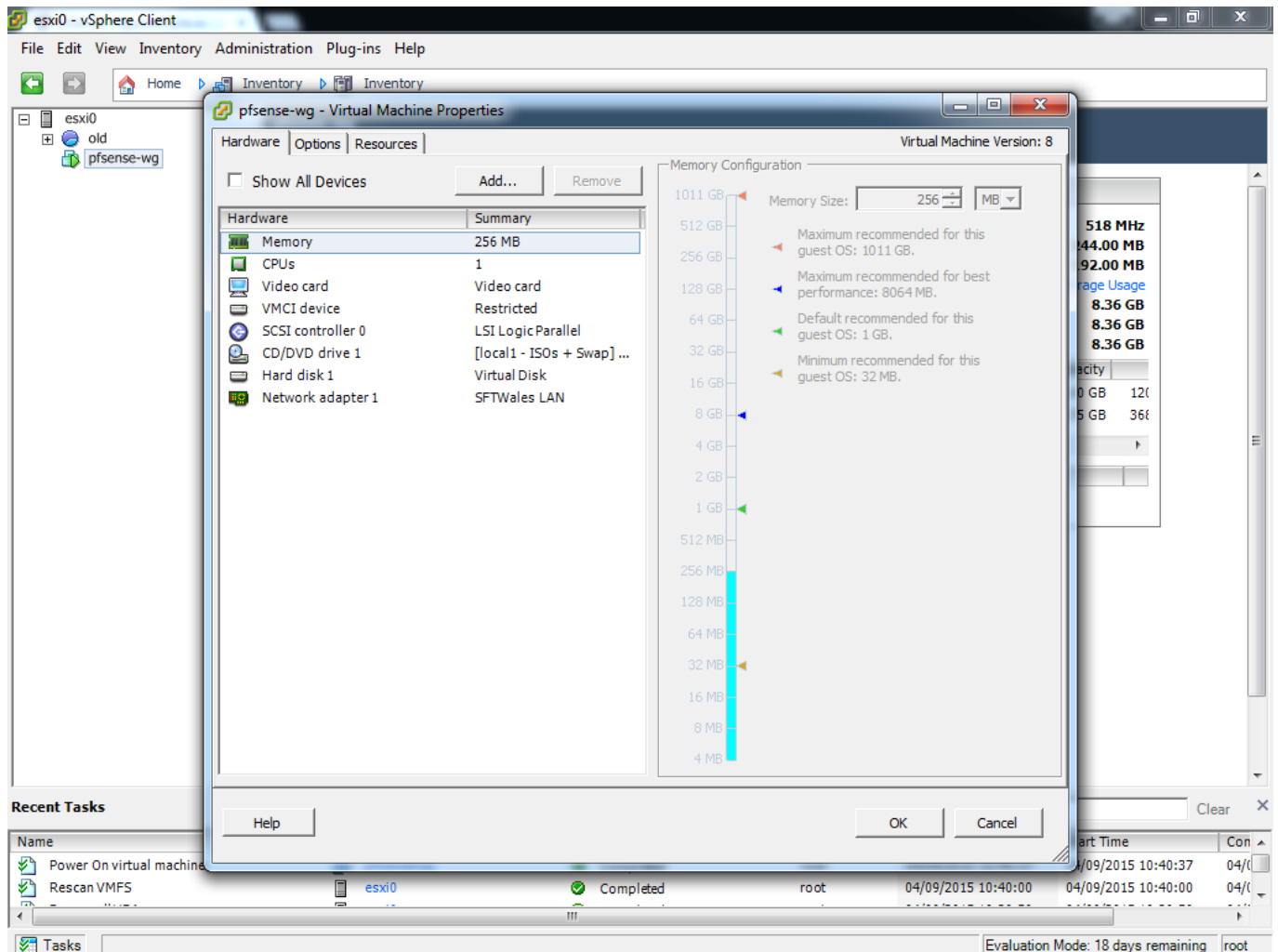
You should see your new 'Virtual Machine Port Group' appear in the Networking section. In this instance you can see 'Walled garden' and it currently connected to a NIC (Physical Adapter) that doesn't have a physical connection. In a production environment you should see this Group assigned to a vSwitch that has a connected NIC before proceeding.

The screenshot shows the vSphere Client interface for an ESXi host. The left sidebar displays the inventory tree with 'esxi0' and 'old' selected. The main pane shows the 'Networking' configuration for the 'Walled garden' VM. The 'View' dropdown is set to 'vSphere Standard Switch'. The 'Networking' section lists several port groups: 'FreeNAS', 'SFTWales LAN', 'FreeNAS', 'pfSense', 'Ubuntu', 'pfsense-wg', 'VMkernel Port', 'VMkernel', 'fd00:190::1', 'Management Network', and 'Walled garden'. The 'Walled garden' port group is highlighted, showing its configuration: 'VMkernel Port', 'vmk1 | VLAN ID: 190', 'fd00:190::1', and 'fe80::250:56ff:fe6e:6b25'. Below the port group list, the 'Standard Switch: vSwitch1' is shown, with a 'Physical Adapters' section containing 'vmnic1'. The 'Recent Tasks' section at the bottom shows a list of tasks with columns for Name, Target, Status, Details, Initiated by, Requested Start Time, Start Time, and Completion Time.

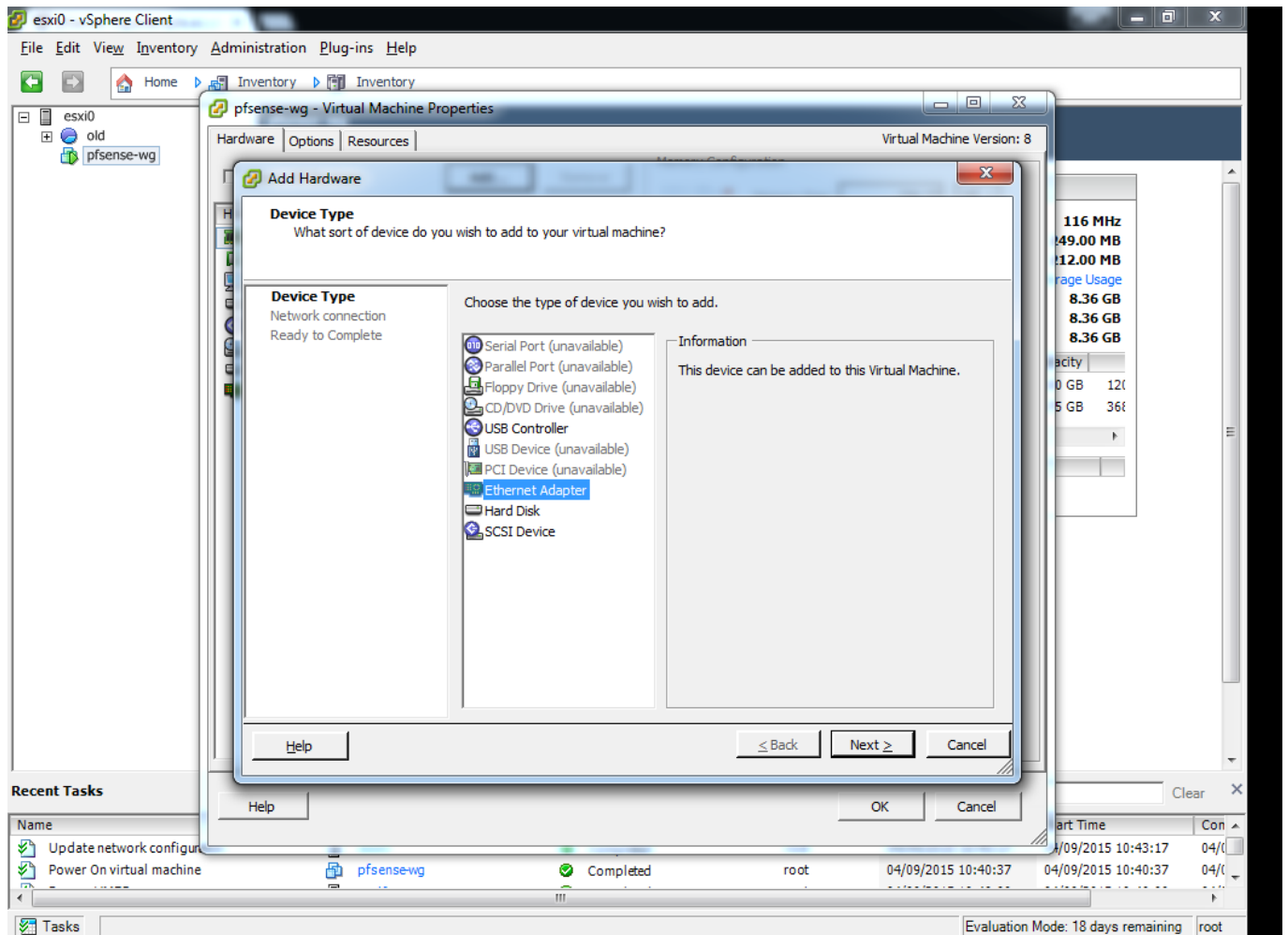
Name	Target	Status	Details	Initiated by	Requested Start Time	Start Time	Completion Time
Update network configuration	esxi0	Completed		root	04/09/2015 10:43:17	04/09/2015 10:43:17	04/09/2015 10:43:17
Power On virtual machine	pfsense-wg	Completed		root	04/09/2015 10:40:37	04/09/2015 10:40:37	04/09/2015 10:40:37

## Virtual Machine Networking Configuration

Click Edit Settings, on the pfSense VM

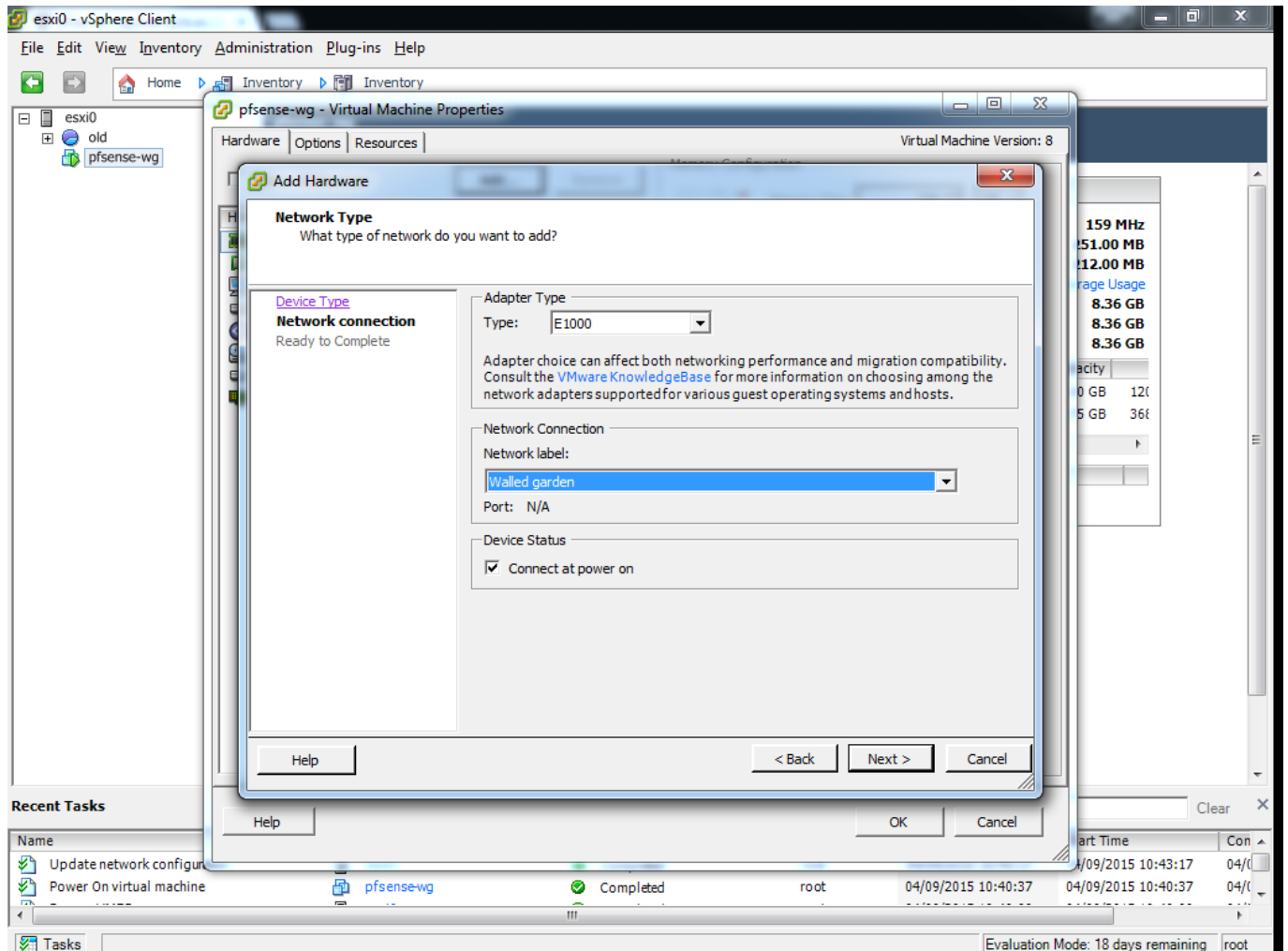


Next Choose Add, and Ethernet Adapter



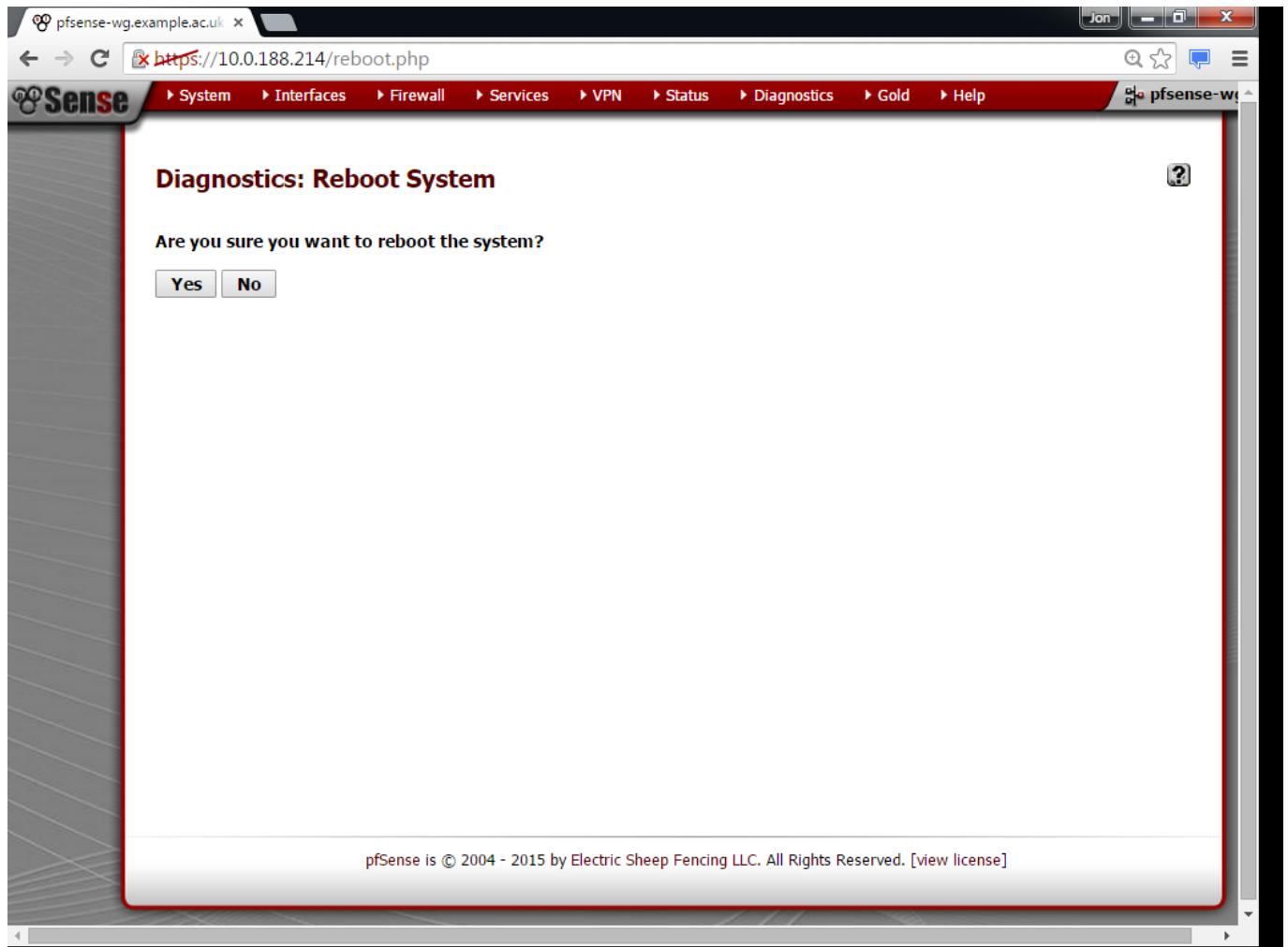
You will be asked to select the Adapter Type, E1000 is the default and can be used with pfSense.

Network Label – here you will choose the Virtual Machine Port group you configured earlier. In this case example we select 'Walled garden'



## Adding the interface into pfSense

Log back into pfSense and choose Reboot system



Following reboot, log back into pfSense via the Web Interface. Before you assign an interface, ensure that you have a Firewall rule that looks like the following to allow HTTPS access on the WAN interface, if it doesn't exist then add one. Otherwise, when you add a new interface pfSense will lock you out, and you will need to connect via the LAN interface ('Walled garden' VLAN)

**Firewall: Rules**

**Floating** **WAN** **WALLEDGARDEN**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 TCP	*	*	This Firewall	443 (HTTPS)	*	none		

☒ pass  
☐ pass (disabled)

☒ match  
☐ match (disabled)

☒ block  
☐ block (disabled)

☒ reject  
☐ reject (disabled)

☒ log  
☐ log (disabled)

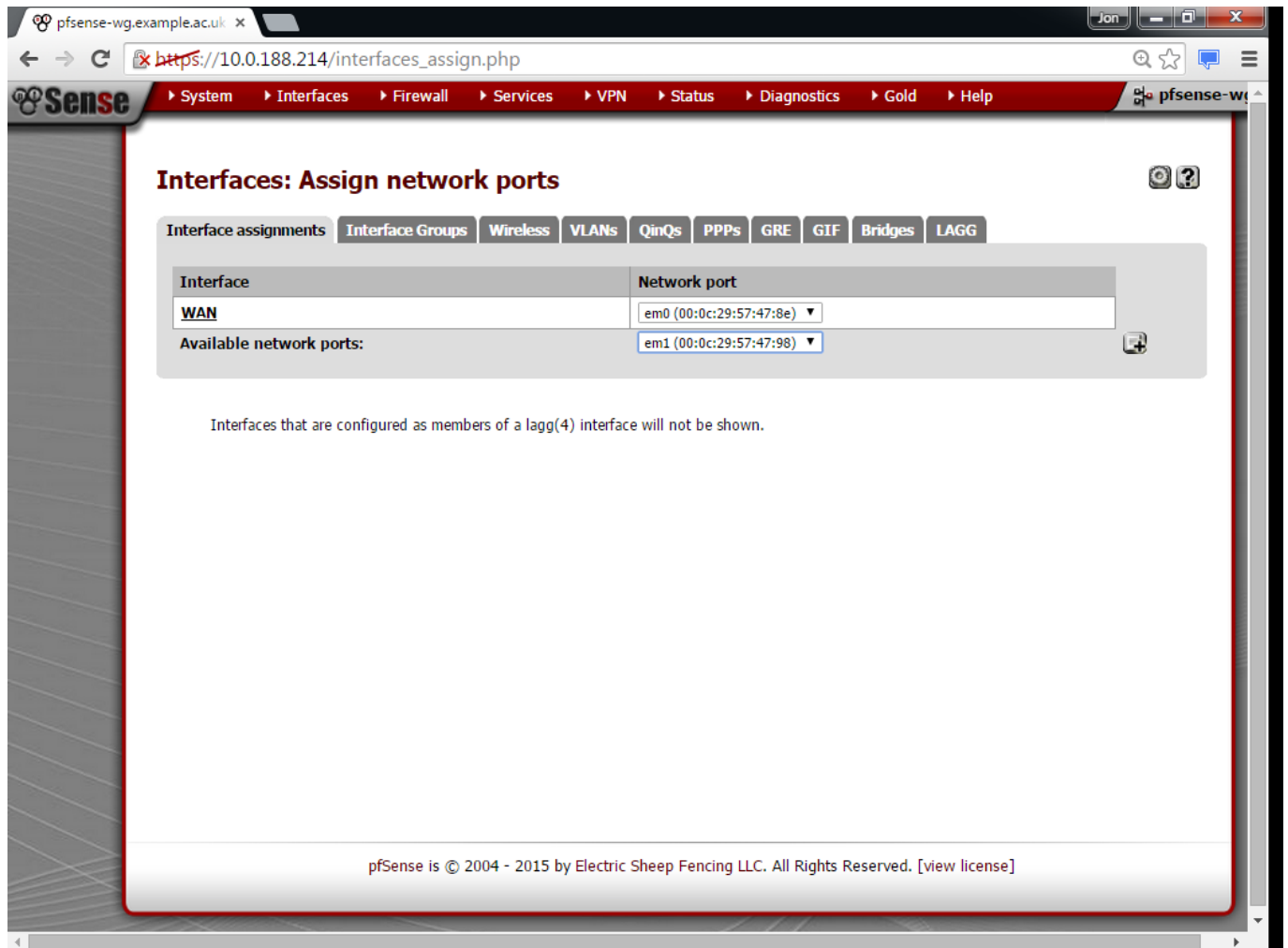
**Hint:**

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]



Now Choose, Interfaces, Assign, You should see an 'Available network port'



Choosing add will create a LAN interface

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

Click on LAN to edit the interface. We would recommend changing the description to something like 'Walled Garden' reflecting the Network Label/VLAN name used on the network. The same can be done for the WAN interface.

The screenshot displays the pfSense web interface for configuring the LAN interface. The browser window shows the URL `https://10.0.188.214/interfaces.php?if=lan`. The page title is "Interfaces: LAN". The "General configuration" section is expanded, showing the following fields:

- Enable:** ☒ Enable Interface
- Description:**  Enter a description (name) for the interface here.
- IPv4 Configuration Type:**
- IPv6 Configuration Type:**
- MAC address:**  This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
- MTU:**  If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
- MSS:**  If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
- Speed and duplex:**  - Show advanced option

The "Private networks" section is also visible, with the following options:

- ☐ **Block private networks**  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.
- ☐ **Block bogon networks**  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by

Next we assign an IP address to the LAN/Walled Garden interface. The IP address and IP subnet should be

- Unique on your network to prevent any unexpected behaviour
- Within one of the IP subnets permitted for use on LANs as per RFC-1918
  - 172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
  - 10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
  - 192.168.0.0 – 192.168.255.255 (192.168.0.0/16)
- We would recommend a minimum of 256 (i.e. a /24) and a maximum of 1024 (/22)
- In this example we use documentation IP address space 198.51.100.254/24 - Do not use this on your LAN!
- It is very unlikely that you will need Public IP address for this solution

The screenshot shows the pfSense web interface for configuring the LAN/Walled Garden interface. The browser address bar shows <https://10.0.188.214/interfaces.php?if=lan>. The interface has a red header with navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Interfaces' and shows the configuration for the 'lan' interface. The 'Static IPv4 configuration' section is expanded, showing the 'IPv4 address' field set to '198.51.100.254' with a '/24' subnet. Below this, the 'IPv4 Upstream Gateway' is set to 'None'. The 'Private networks' section is also expanded, showing two checkboxes: 'Block private networks' and 'Block bogon networks', both of which are unchecked. A note at the bottom of the 'Private networks' section states: 'Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.' At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Next reconfigure the DHCP server. By going to Services, DHCP. You will need to enter the IP range to be assigned via DHCP.

Generally you can assign almost the complete 'Available range'. We would recommend keeping some IPs free if you are aware that your wireless controller(s) require SVIs (Meru and Cisco do).

The screenshot shows the pfSense web interface for configuring the DHCP server on the WALLEDGARDEN interface. The browser address bar shows [https://10.0.188.214/services\\_dhcp.php](https://10.0.188.214/services_dhcp.php). The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main heading is "Services: DHCP server". A red error message box states: "The following input errors were detected: The field Range begin is required. The field Range end is required." The configuration section for WALLEDGARDEN includes a checkbox for "Enable DHCP server on WALLEDGARDEN interface" (checked), a checkbox for "Deny unknown clients" (unchecked), and a note: "If this is checked, only the clients defined below will get DHCP leases from this server." The Subnet is 198.51.100.0 and the Subnet mask is 255.255.255.0. The Available range is 198.51.100.1 - 198.51.100.254. The Range is set to 198.51.100.1 to 198.51.100.250. There is a section for Additional Pools with a table for Pool Start, Pool End, and Description. Below this are sections for WINS servers and DNS servers, each with three input fields.

Pool Start	Pool End	Description

WINS servers

DNS servers

## Captive Portal configuration

Under Services, you will find Captive Portal

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The 'Services' menu is expanded, showing options like Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server/RA, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP proxy, Load Balancer, NTP, PPPoE Server, SNMP, UPnP & NAT-PMP, and Wake on LAN. The 'Captive Portal' option is highlighted. The main content area is titled 'Services: DHCP server' and shows the configuration for the 'WALLEDGARDEN' interface. The 'Enable' checkbox is checked. Below this, there are fields for Subnet (198.51.100.0), Subnet mask (255.255.255.0), Available range (198.51.100.0), and Range (198.51.100.0 to 198.51.100.250). A table for 'Additional Pools' is shown with columns for Pool Start, Pool End, and Description. There are also fields for WINS servers, DNS servers, and Gateway. A note at the bottom states: 'NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.'

Choose to add a Captive Portal Zone, and you will be presented with the following window. Note the restriction around zone names.

The screenshot shows a web browser window with the URL `https://10.0.188.214/services_captiveportal_zones_edit.php`. The browser's address bar also shows `pfsense-wg.example.ac.uk`. The page title is "Services: Captive portal: Edit Zones". The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Edit Captive Portal Zones" and contains a form with two fields: "Zone name" and "Description". The "Zone name" field has a tooltip that says "Zone name. Can only contain letters, digits, and underscores (\_)." The "Description" field has a tooltip that says "You may enter a description here for your reference (not parsed)." There is a "Continue" button at the bottom of the form. The footer of the page states "pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]".

**Services: Captive portal: Edit Zones**

**Edit Captive Portal Zones**

Zone name	<input type="text"/>
Zone name. Can only contain letters, digits, and underscores (_).	
Description	<input type="text"/>
You may enter a description here for your reference (not parsed).	

[Continue](#)

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [\[view license\]](#)

This is the main captive portal configuration page.

Under Interfaces

Choose the appropriate interface. In this case we have named the interface concerned 'WALLEDGARDEN'

The screenshot shows the pfSense web interface for configuring a captive portal. The browser address bar shows `https://10.0.188.214/services_captiveportal.php?zone=walledgarden`. The page title is "Services: Captive portal: walledgarden". The "Captive portal(s)" tab is selected, showing a list of tabs: "Captive portal(s)", "MAC", "Allowed IP addresses", "Allowed Hostnames", "Vouchers", and "File Manager". The "Enable captive portal" checkbox is checked. The "Interfaces" dropdown menu is set to "WALLEDGARDEN". The "Maximum concurrent connections" field is set to 100, with a note that this limits the number of concurrent connections to the captive portal HTTP(S) server. The "Idle timeout" field is set to 10 minutes. The "Hard timeout" field is set to 10 minutes. The "Pass-through credits allowed per MAC address" field is set to 10, with a note that this allows passing through the captive portal without authentication a limited number of times per MAC address. The "Waiting period to restore pass-through credits" field is set to 1 hour. The "Reset waiting period on attempted access" checkbox is unchecked. The "Logout popup window" checkbox is unchecked.

Services: Captive portal: walledgarden

Captive portal(s) MAC Allowed IP addresses Allowed Hostnames Vouchers File Manager

☒ Enable captive portal

Interfaces: WAN, WALLEDGARDEN (selected)  
Select the interface(s) to enable for captive portal.

Maximum concurrent connections: 100 per client IP address (0 = no limit)  
This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.

Idle timeout: 10 minutes  
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout: 10 minutes  
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Pass-through credits allowed per MAC address: 10 per client MAC address (0 or blank = none)  
This setting allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Waiting period to restore pass-through credits: 1 hours  
Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period on attempted access: ☐ Enable waiting period reset on attempted access  
If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window: ☐ Enable logout popup window



Under Pre-authentication redirect URL – you should insert the help page you wish to use for your Walled Garden, this could be a direct link to eduroam CAT, as suggested below, but maybe your organisations eduroam support webpage.

The screenshot shows the pfSense captive portal configuration page for the 'walledgarden' zone. The page is titled 'pfsense-wg' and has a navigation menu with links to System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is divided into several sections, each with a title and a description of the setting. The settings are as follows:

- Waiting period to restore pass-through credits:** A text input field with the value '0' and a unit of 'hours'. The description states: 'Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.'
- Reset waiting period on attempted access:** A checkbox labeled 'Enable waiting period reset on attempted access'. The description states: 'If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.'
- Logout popup window:** A checkbox labeled 'Enable logout popup window'. The description states: 'If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.'
- Pre-authentication redirect URL:** A text input field with the value 'https://cat.eduroam.org/?idp=967'. The description states: 'Use this field to set \$PORTAL\_REDIRECTURL\$ variable which can be accessed using your custom captive portal index.php page or error pages.'
- After authentication Redirection URL:** A text input field with the value 'https://cat.eduroam.org/?idp=967'. The description states: 'If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.'
- Blocked MAC address redirect URL:** A text input field with the value 'https://cat.eduroam.org/?idp=967'. The description states: 'If you provide a URL here, MAC addresses set to be blocked will be redirect to that URL when attempt to access anything.'
- Concurrent user logins:** A checkbox labeled 'Disable concurrent logins'. The description states: 'If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.'
- MAC filtering:** A checkbox labeled 'Disable MAC filtering'. The description states: 'If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.'
- Pass-through MAC Auto Entry:** Two checkboxes: 'Enable Pass-through MAC automatic additions' and 'Enable Pass-through MAC automatic addition with username'. The description for the first checkbox states: 'If this option is set, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry you either have to log in and remove it manually from the MAC tab or send a POST from another system to remove it. If this is enabled, RADIUS MAC authentication cannot be used. Also, the logout window will not be shown.'

Under 'portal contents page', you will need to select 'Choose file'... At this point it would state 'No file chosen'

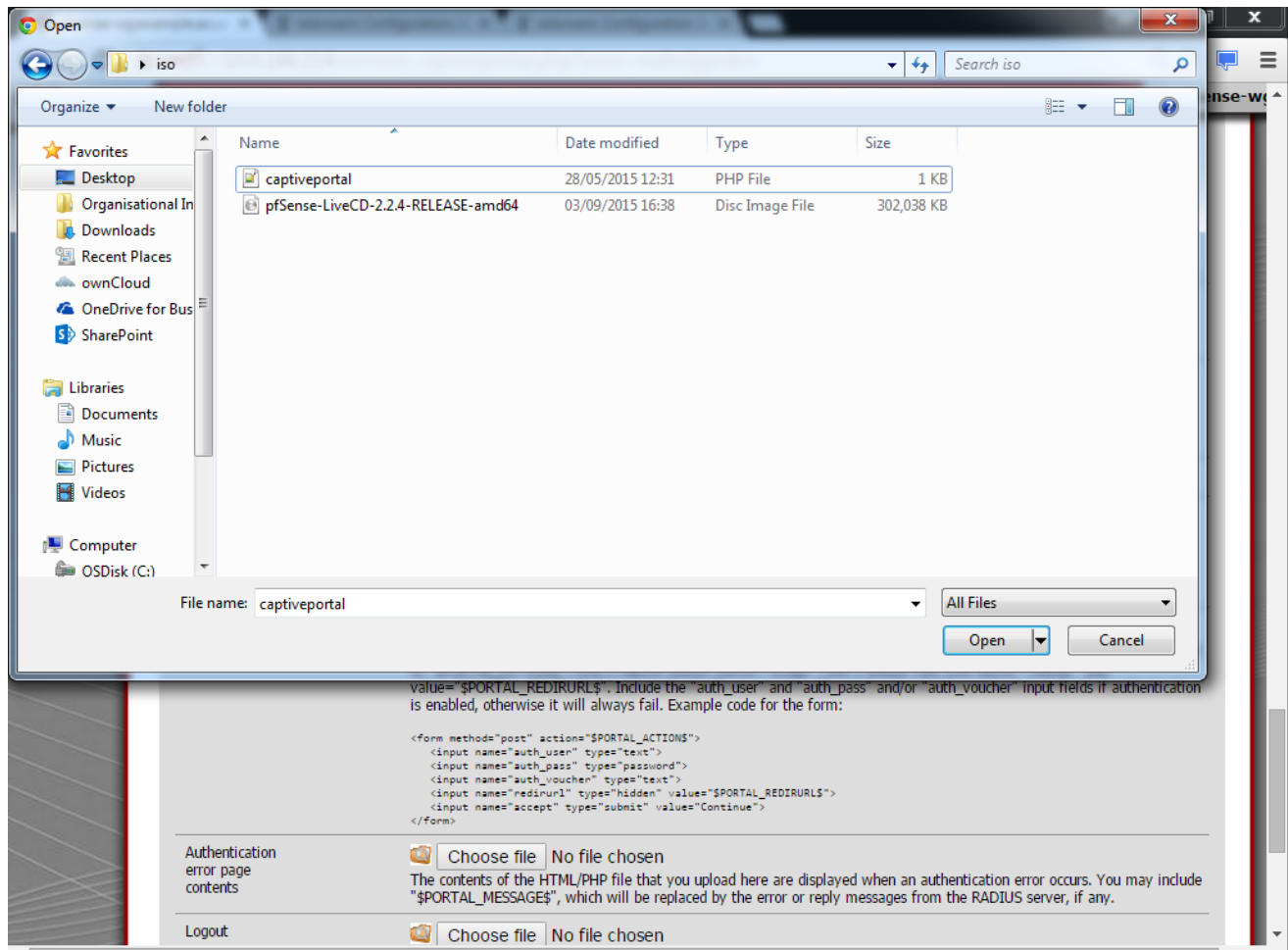
The screenshot shows the pfSense web interface for configuring the captive portal. The browser address bar shows `https://10.0.188.214/services_captiveportal.php?zone=walledgarden`. The interface has a top navigation bar with links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Specify a NAS identifier to override the default value (pfsense-wg.example.ac.uk)'.

The configuration options include:

- MAC address format:** A dropdown menu set to 'default'. Below it, a text box explains that this option changes the MAC address format used in the whole RADIUS system. It lists several formats: default (00:11:22:33:44:55), singledash (001122-334455), ietf (00-11-22-33-44-55), cisco (0011.2233.4455), and unformatted (001122334455).
- HTTPS login:** A checkbox labeled 'Enable HTTPS login'. Below it, a text box explains that if enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.
- HTTPS server name:** A text input field. Below it, a text box explains that this name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.
- SSL Certificate:** A dropdown menu set to 'webConfigurator default (55e86d4723f83)'.
- Disable HTTPS forwards:** A checkbox labeled 'Disable HTTPS forwards'. Below it, a text box explains that if this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.
- Portal page contents:** A section with a 'Choose file' button and the filename 'captiveportal.php'. Below it, a text box explains that you should upload an HTML/PHP file for the portal page here (leave blank to keep the current one). It provides instructions on the form structure, including a submit button and hidden fields for redirection. Example code is provided: 

```
<form method="post" action="$PORTAL_ACTIONS">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL">
  <input name="accept" type="submit" value="Continue">
</form>
```
- Authentication error page contents:** A section with a 'Choose file' button and the text 'No file chosen'. Below it, a text box explains that the contents of the HTML/PHP file that you upload here are displayed when an authentication error occurs. You may include "\$PORTAL\_MESSAGES", which will be replaced by the error or reply messages from the RADIUS server, if any.
- Logout:** A section with a 'Choose file' button and the text 'No file chosen'.

Under preparation you should have downloaded the **RAW (PHP) version** of the following code from **Gist/GitHub**. In the example below it is the 'captiveportal.php' file on the local machine.



Under portal page contents, you should now see captiveportal.php listed

pfSense-wg.example.ac.uk x eduroam Configuration A x eduroam Configuration A x Jon

https://10.0.188.214/services\_captiveportal.php?zone=walledgarden

Sense System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Specify a NAS identifier to override the default value (pfSense-wg.example.ac.uk)

MAC address format: default

This option changes the MAC address format used in the whole RADIUS system. Change this if you also need to change the username format for RADIUS MAC authentication.

default: 00:11:22:33:44:55  
singledash: 001122-334455  
ietf: 00-11-22-33-44-55  
cisco: 0011.2233.4455  
unformatted: 001122334455

HTTPS login: ☐ Enable HTTPS login

If enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name:

This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL Certificate: webConfigurator default (55e86d4723f83)

Disable HTTPS forwards: ☐ Disable HTTPS forwards

If this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

Portal page contents: Choose file captiveportal.php

Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL\_ACTIONS\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL\_REDIRURL\$". Include the "auth\_user" and "auth\_pass" and/or "auth\_voucher" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="auth_voucher" type="text">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
  <input name="accept" type="submit" value="Continue">
</form>
```

Authentication error page contents: Choose file No file chosen

The contents of the HTML/PHP file that you upload here are displayed when an authentication error occurs. You may include "\$PORTAL\_MESSAGES\$", which will be replaced by the error or reply messages from the RADIUS server, if any.

Logout: Choose file No file chosen

Under the Allow Hostnames tab, you should now be able to add hostnames of websites which you want to be accessible via the Walled Garden. The next section discusses this further.

The screenshot shows the pfSense web interface for configuring the 'walledgarden' captive portal. The 'Allowed Hostnames' tab is active, displaying a table with the following content:

Hostname	Description
<input checked="" type="checkbox"/> cat.eduroam.org	

**Note:**  
Adding allowed Hostnames will allow a DNS hostname access to/from access through the captive portal without being taken to the portal page. This can be used for a web server serving images for the portal page or a DNS server on another network, for example. By specifying *from* addresses, it may be used to always allow pass-through access from a client behind the captive portal.

any ► x.x.x.x All connections **to** the Hostname are allowed  
x.x.x.x ► any All connections **from** the Hostname are allowed  
☒ All connections **to** and **from** the Hostname are allowed

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

## Configuring allowed websites

We would suggest the following as a minimum;

- The 'Required' list from the **eduroam CAT (Configuration Assistance Tool)** website (the list is recreated in the next section)
- Your organisations eduroam support web page.
- eduroam support web page of any partners who may make regular use of your network.

Note: webpages will be available over an open public Wi-Fi network, and so you should avoid sites that may pass sensitive information e.g. authentication, and pay close attention to any sites which may open up wider access e.g. Google which are part of the recommendations from eduroam CAT

## eduroam CAT website list

The following are a list of websites that should be opened via a walled garden. These are taken directly from the eduroam CAT website, and are available on the 'About eduroam CAT' link. The screenshot and tables below were taken on 6<sup>th</sup> July 2016.

### Screenshot

**eduroam CAT** is publicly accessible. To enable its use behind captive portals (e.g. on a 'setup' SSID which only allows access to CAT for device configuration), the following hostnames need to be allowed for port TCP/443 in the portal:

#### REQUIRED

- **cat.eduroam.org** (the service itself)
- **crl3.digicert.com, crl4.digicert.com** (the CRL Distribution Points for the site certificate), also TCP/80
- **ocsp.digicert.com** (the OCSP Responder for the site certificate), also TCP/80
- **android.l.google.com** (Google Play access for Android App)
- **android.clients.google.com** (Google Play access for Android App)
- **play.google.com** (Google Play access for Android App)
- **ggpht.com** (Google Play access for Android App)

**RECOMMENDED** for full Google Play functionality (otherwise, Play Store will look broken to users and/or some non-vital functionality will not be available)

- **photos-ugc.l.google.com**
- **googleusercontent.com**
- **ajax.googleapis.com**
- **play.googleapis.com**
- **googleapis.l.google.com**
- **apis.google.com**
- **gstatic.com**
- **www.google-analytics.com**
- **wallet.google.com**
- **plus.google.com**
- **checkout.google.com**

### Lists

Required	Recommended
cat.eduroam.org	photos-ugc.l.google.com
crl3.digicert.com	googleusercontent.com
crl4.digicert.com	ajax.googleapis.com
ocsp.digicert.com	play.googleapis.com
android.l.google.com	googleapis.l.google.com
android.clients.google.com	apis.google.com
play.google.com	gstatic.com
ggpht.com	www.google-analytics.com
	wallet.google.com
	plus.google.com
	checkout.google.com

## Installing Open VM Tools

If you have installed into VMware then you should install the VMware tools. In this case we use the Open VM Tools which are available as package within pfSense.

Choose System, and Packages

The screenshot shows the pfSense web interface at the URL <https://10.0.188.219/index.php>. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The left sidebar menu is open, showing options like Advanced, Cert Manager, Firmware, General Setup, High Avail. Sync, Logout, Packages, Routing, Setup Wizard, and User Manager. The main content area displays the 'Dashboard' with various system statistics and the 'Interfaces' section.

**System Information:**

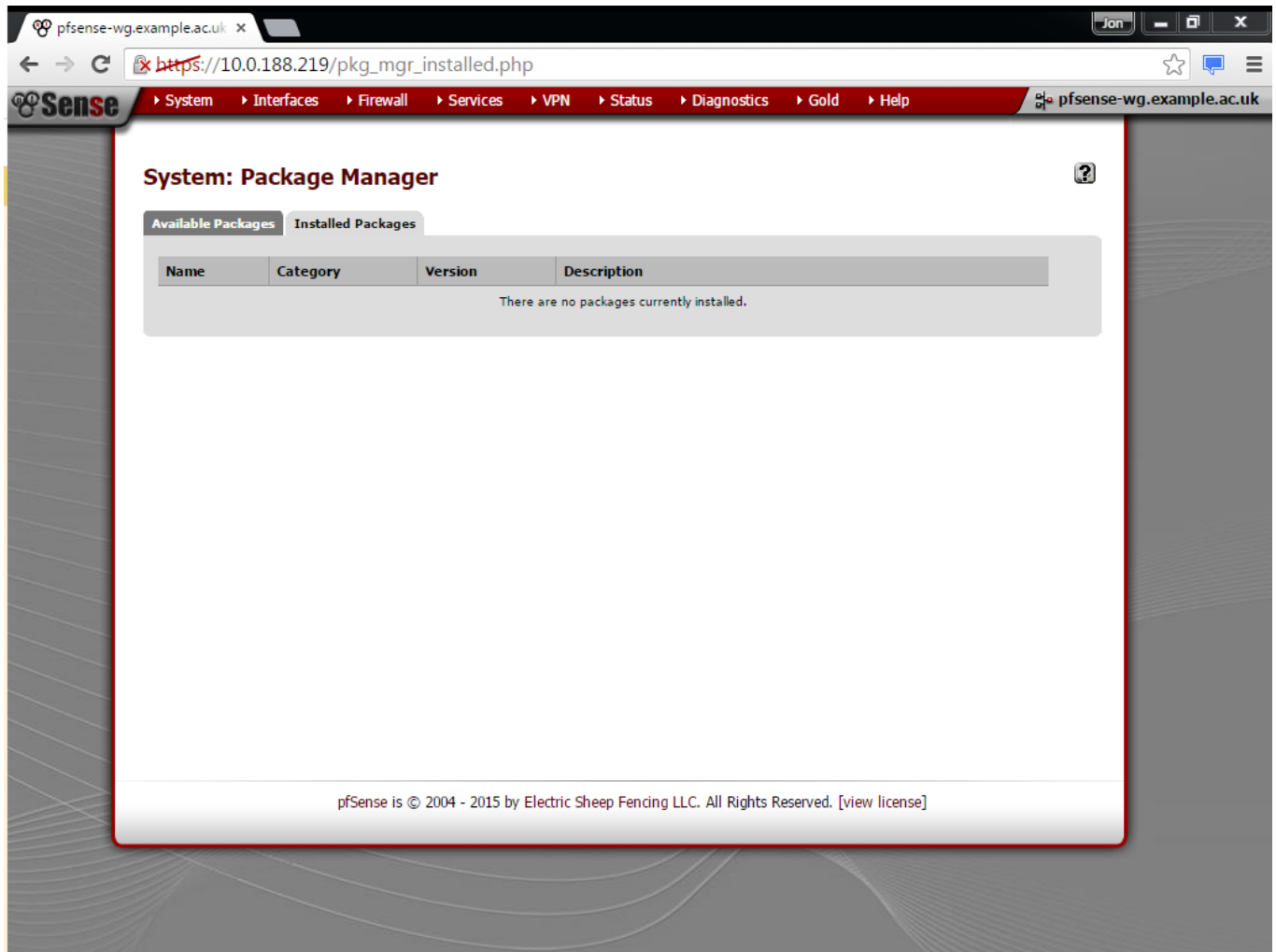
- Platform: pfSense
- CPU Type: Intel(R) Xeon(R) CPU 3065 @ 2.33GHz
- Uptime: 00 Hour 08 Minutes 34 Seconds
- Current date/time: Thu Oct 29 15:23:28 GMT 2015
- DNS server(s): 127.0.0.1, 10.0.188.253, 10.0.188.1, 8.8.8.8, 8.8.4.4
- Last config change: Thu Oct 29 15:19:37 GMT 2015
- State table size: 0% (27/22000)
- MBUF Usage: 8% (1086/14112)
- Load average: 0.13, 0.24, 0.16
- CPU usage: (Updating in 10 seconds)
- Memory usage: 66% of 221 MB
- SWAP usage: 1% of 511 MB

**Interfaces:**

Interface	Speed	MAC Address	IP Address
WAN (DHCP)	1000baseT <full-duplex>	10.0.188.219 2a01:348:2cd:bc:20c:29ff:fe57:478e	
WALLEDGARDEN	1000baseT <full-duplex>	198.51.100.254	



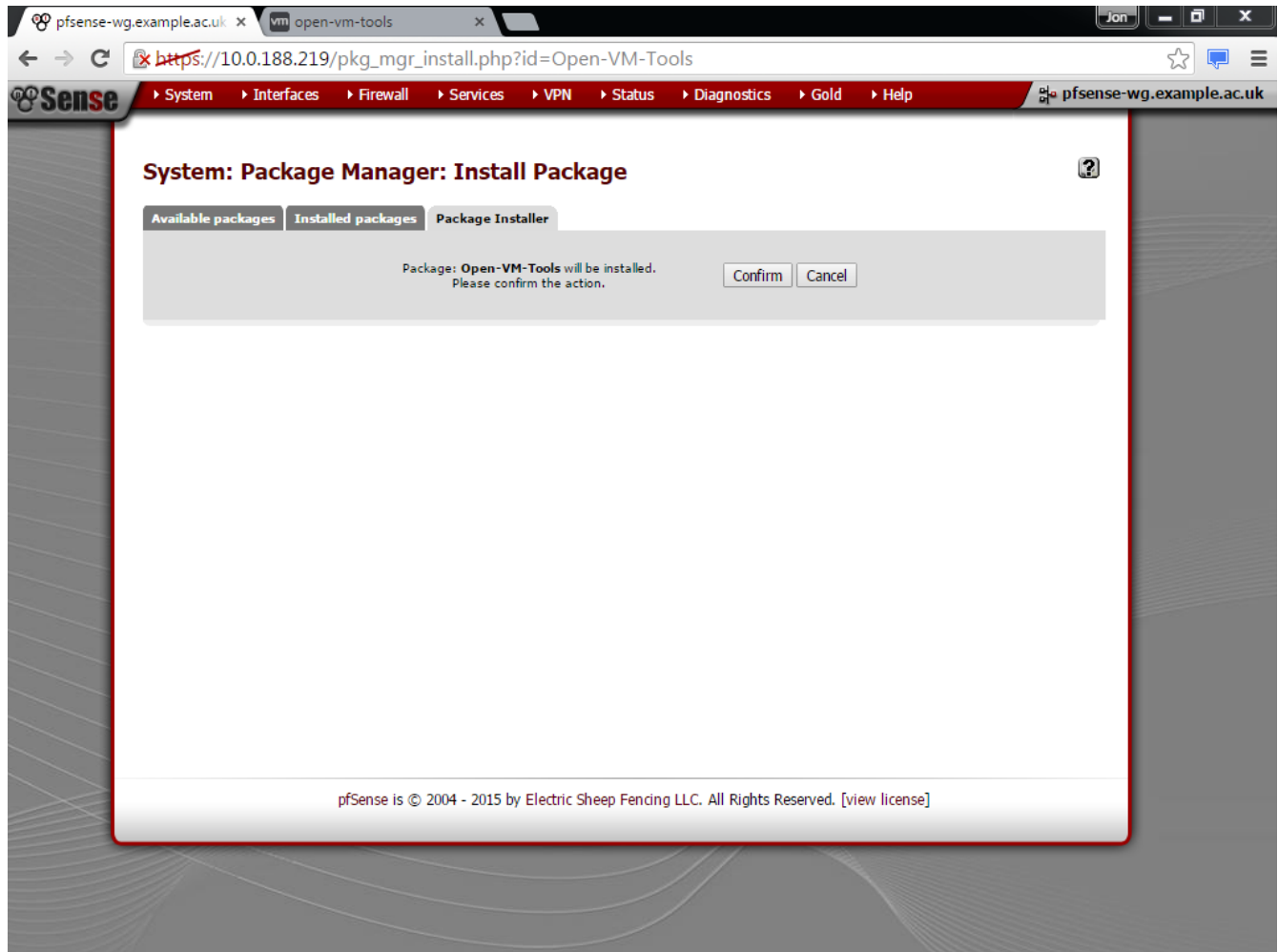
From within Package Manager choose Available Packages.



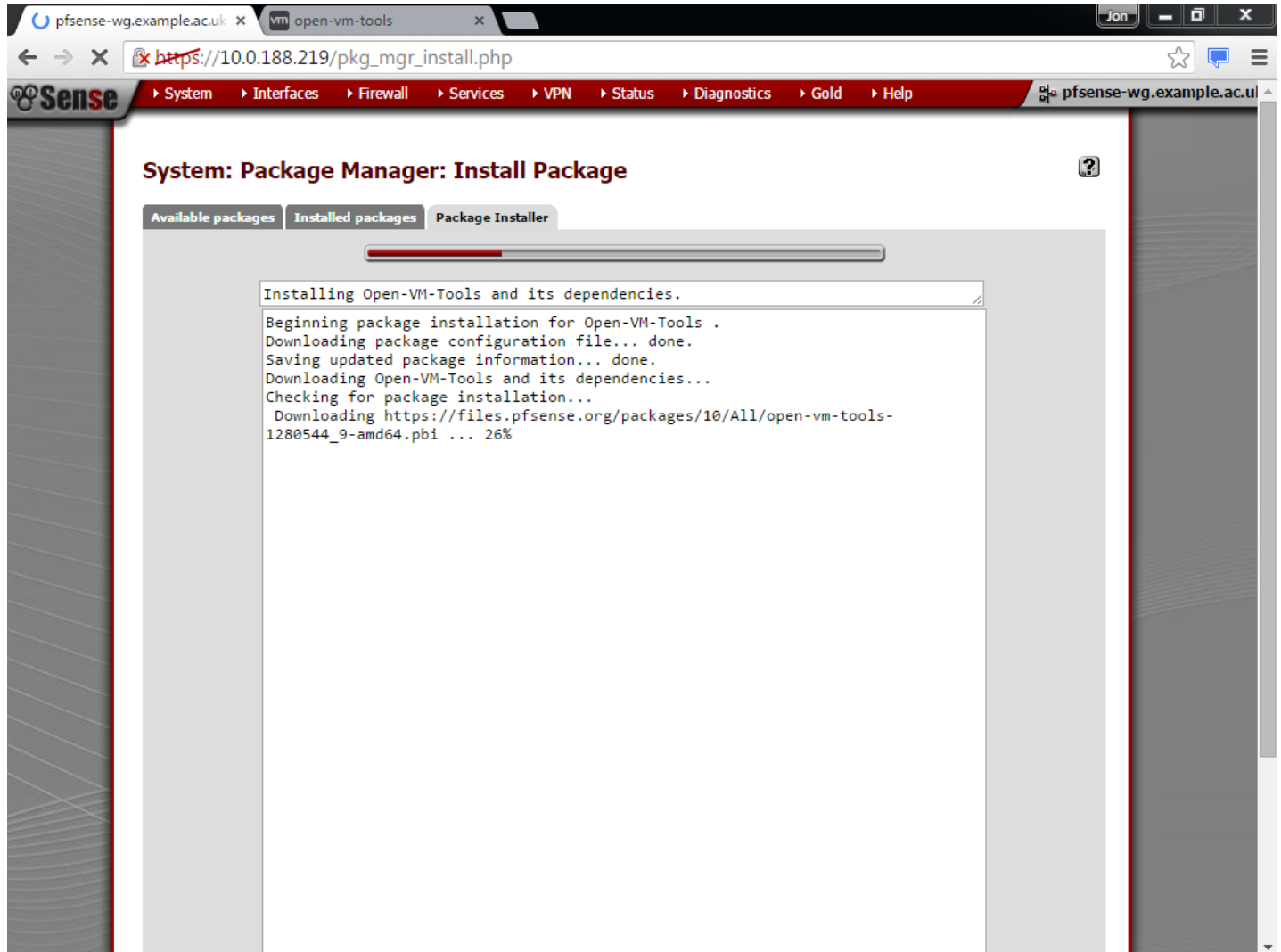
You will find Open-VM-Tools in the All Packages list. Once located Choose the Install button on the right hand side.

Package Name	Category	Version	Platform	Description	Action
ntopng	Network Management	BETA 0.8.1	platform: 2.2	ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.	Install
nut	Network Management	BETA 2.1.1	platform: 2.2 2.2.999	Network UPS Tools.	Install
olsrd	Services	Stable 1.0.3	platform: 2.2 2.2.999	The olsr.org OLSR daemon is an implementation of the Optimized Link State Routing protocol. OLSR is a routing protocol for mobile ad-hoc networks. The protocol is pro-active, table driven and utilizes a technique called multipoint relaying for message flooding.	Install
Open-VM-Tools	Services	Stable 1280544.12	platform: 2.2	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	Install
OpenBGPD	NET	STABLE 0.9.3.8	platform: 2.2	OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. <b>WARNING! Installs files to the same place as Quagga OSPF. Installing both will result in a broken state, remove this package before installing Quagga OSPF.</b>	Install
OpenVPN Client Export Utility	Security	RELEASE 1.2.20	platform: 2.2	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	Install
pfBlockerNG	Firewall	Stable 1.10	platform: 2.2	pfBlockerNG is the Next Generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. Country Blocking Database by MaxMind Inc. (GeoLite Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Emerging Threats IQRisk IP Reputation Threat Sources.	Install

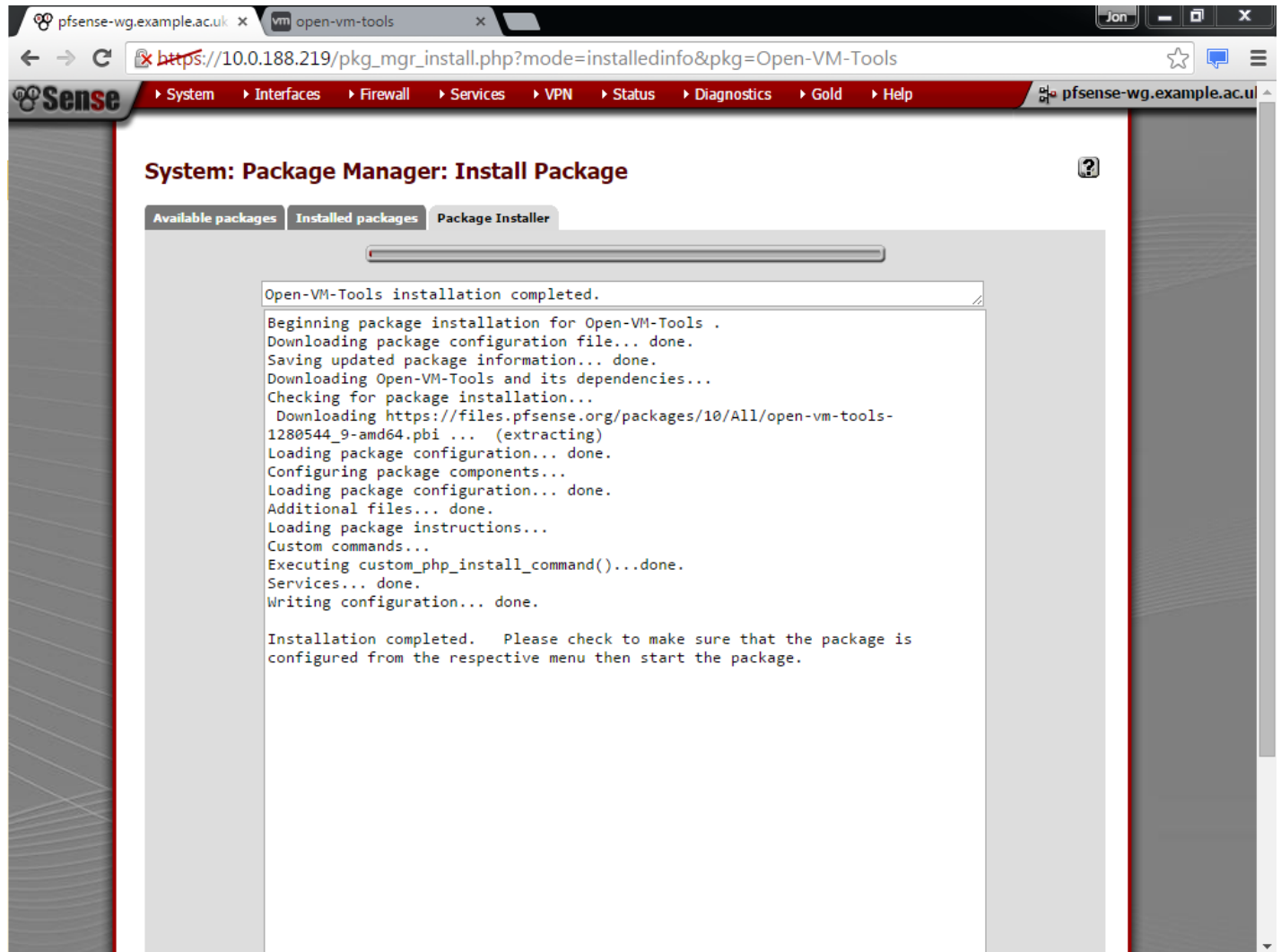
Choose Confirm



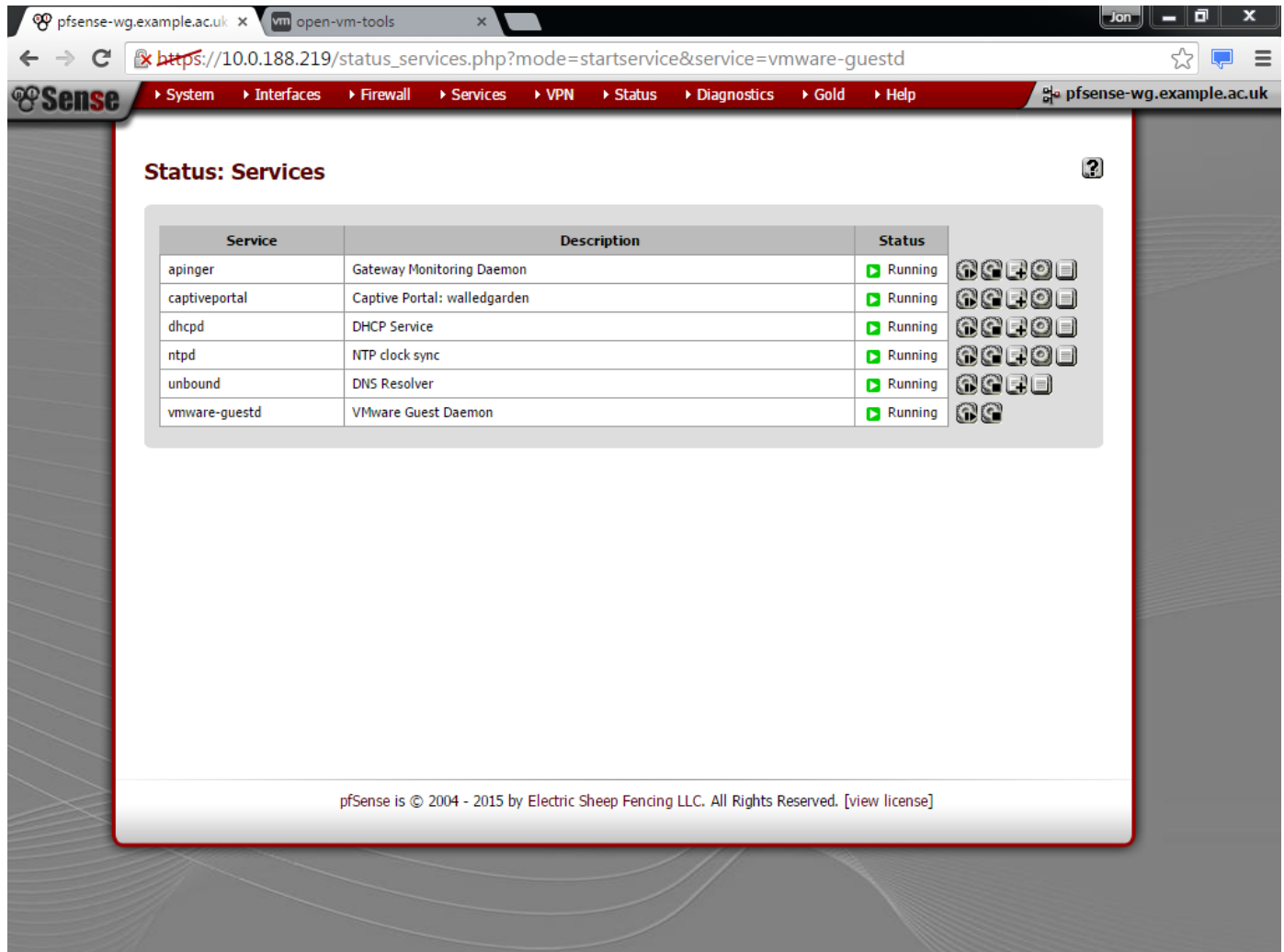
This is the Open-VM-Tools package installing...



Once the Open-VM-Tools package is complete, you will see 'Installation completed'.



You should check that that Open-VM-Tools (vmware-guestd) is running by choosing Status, Services.



The screenshot shows the pfSense web interface. The browser address bar displays `https://10.0.188.219/status_services.php?mode=startservice&service=vmware-guestd`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Status: Services" and contains a table with the following data:

Service	Description	Status
apinger	Gateway Monitoring Daemon	Running
captiveportal	Captive Portal: walledgarden	Running
dhcpd	DHCP Service	Running
ntpd	NTP clock sync	Running
unbound	DNS Resolver	Running
vmware-guestd	VMware Guest Daemon	Running

At the bottom of the page, a copyright notice states: "pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]"

You should also check that the underlying VMware Hypervisor/Virtualisation Software sees that Tools are now installed. As you can see it reports 'Running (3<sup>rd</sup>-party/Independent)'.

The screenshot shows the vSphere Client interface for a VM named 'pfsense-wg'. The left sidebar shows the inventory tree with 'esxi0' as the host, containing 'FreeNAS', 'Powered off VMs', 'VMs', and 'pfsense-wg'. The main panel displays the 'Summary' tab for 'pfsense-wg'.

**General**

- Guest OS: FreeBSD (64-bit)
- VM Version: 8
- CPU: 1 vCPU
- Memory: 256 MB
- Memory Overhead: 49.98 MB
- VMware Tools: ② Running (3rd-party/Independent)
- IP Addresses: 10.0.188.219 [View all](#)
- DNS Name: pfsense-wg.example.ac.uk
- State: Powered On
- Host: esxi0.private.sftwales.com
- Active Tasks:
- vSphere HA Protection: ② N/A

**Commands**

- Shut Down Guest
- Suspend
- Restart Guest
- Edit Settings
- Open Console

**Annotations**

Notes: [Edit](#)

**Resources**

Consumed Host CPU: **83 MHz**  
Consumed Host Memory: **295.00 MB**  
Active Guest Memory: **199.00 MB** [Refresh Storage Usage](#)

Provisioned Storage: **8.36 GB**  
Not-shared Storage: **8.36 GB**  
Used Storage: **8.36 GB**

Storage	Drive Type	Capacity	Free Space
local1 - ISOs + S...	Non-SSD	149.00 GB	36.00 GB
vm-storage	SSD	379.75 GB	32.00 GB

**Network**

Network	Type
Walled garden	Standard port group
SFTWales LAN	Standard port group

Tasks: [Evaluation Mode: 11 days remaining](#) root

## Access Point configuration

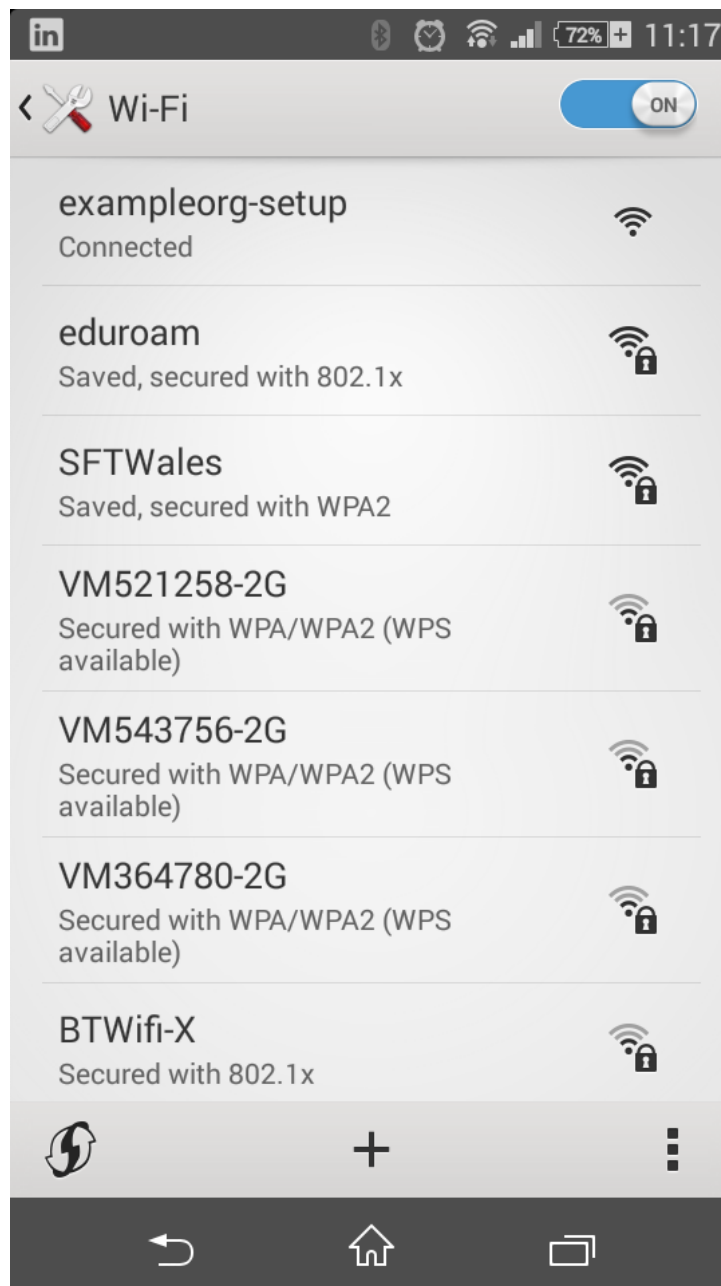
There are many access points and potential configurations that you may have. The following points should assist you in considering those steps

- For VM installations (particularly VMWare)
  - Ensure that you have added the Walled Garden VLAN to all VMware Servers in your Cluster, and across all interfaces that connect to that vSwitch.
  - Ensure that all interfaces between the VMware Nodes (Hypervisors) have added the Walled Garden VLAN to all Switch ports that connect with VMware.
    - These can be problematic to trace. Neighbour discovery protocols such as LLDP and CDP can help here.
- For physical installations
  - Ensure that you have added the Walled Garden VLAN to the LAN port of the pfSense device/server. You will (unless you configured VLANs in pfSense) need to use a port with no 802.1q VLAN tagging in place (untagged / access VLAN)
- For all installations
  - Ensure that the Walled Garden VLAN is tagged between the pfSense server/VM and your Access Point or Access Point Controller.
  - Create a single Open SSID with no authentication, and ensure that it allocates devices to the Walled Garden VLAN.
  - For this Open SSID ensure that Client Isolation is turned on, such that devices can only communicate with the pfSense LAN interface within the Walled Garden VLAN, and not with each other

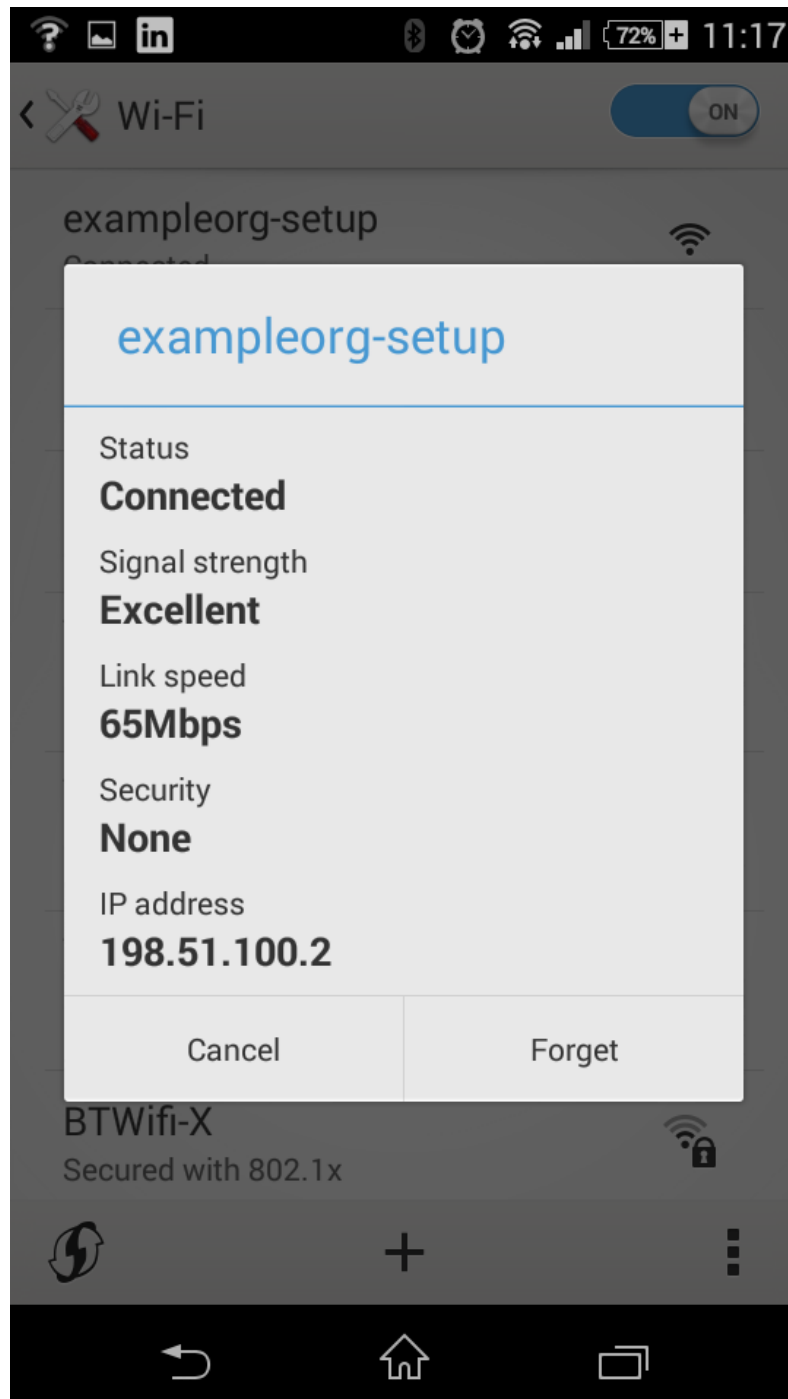


## Testing the user experience

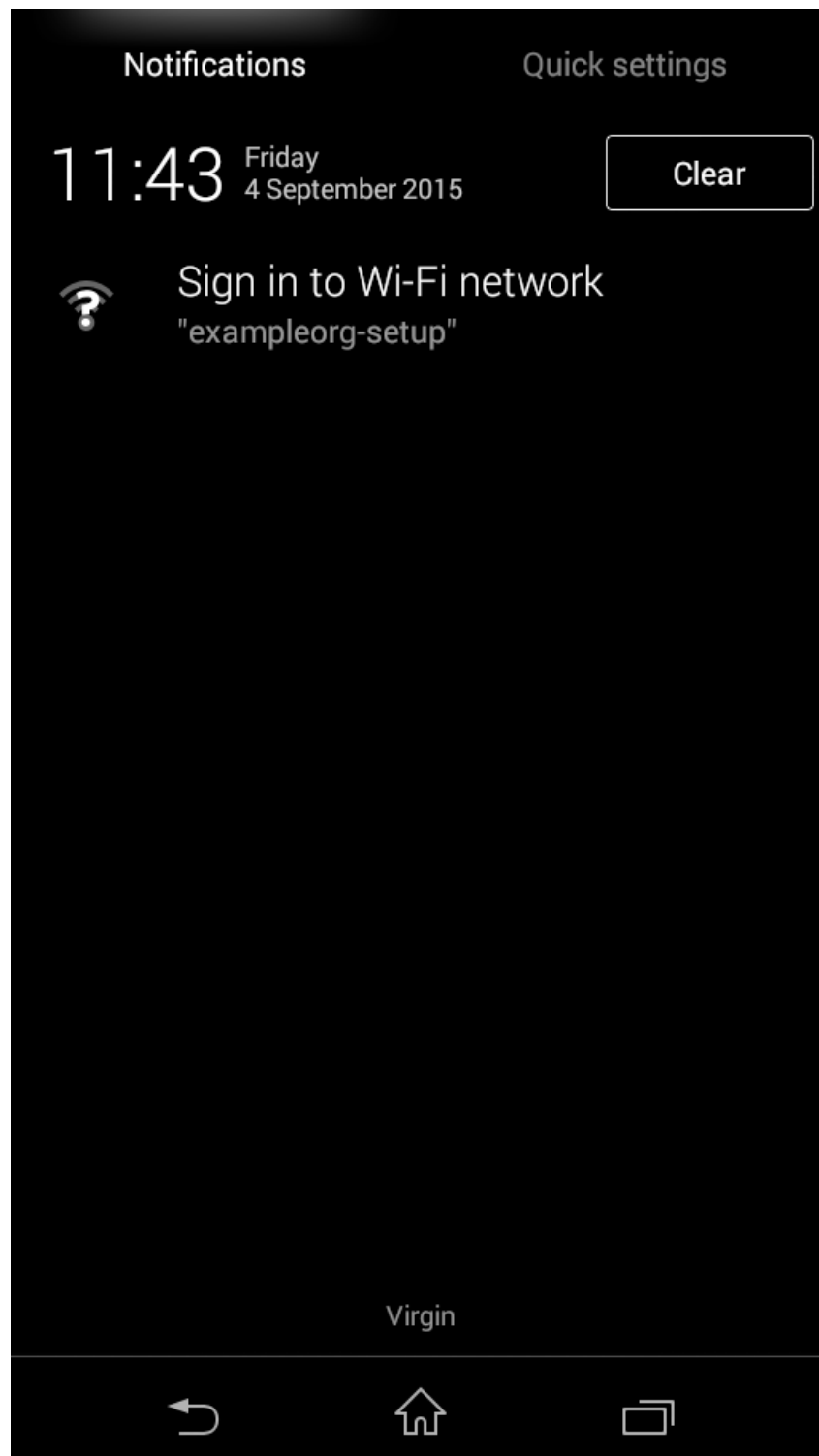
This is an example from an Android device; the user will see an open network – in this case 'exampleorg-setup'. You must not call this 'eduroam-setup' as it violates the **eduroam(UK) Technical specification**, ideally you should put your organisation name (or a fairly unique derivative of that your users will recognise)



Once connected they should receive an IP address. Ensure this is consistent with what you have configured within pfSense on the LAN interface.



Many device operating systems and browsers will detect that they are in a captive portal and ask users to 'Sign into Wi-Fi' this should redirect them to your help page or the eduroam CAT page for your organisation.



This is an example of a device being directed to your help page or the eduroam CAT page for your organisation.

