CIS 76 VLab Pod Setup

Last updated 11/30/2016

Status on setup instructions:

1. pfSense (2.3.1, 64 bit) - OK
2. Kali (2016.1, 64 bit) - OK
3. Windows XP (SP2, 32 bit) - OK
4. Port Forwarding - OK
5. OWASP_Broken_Web_Apps_VM_1.2 - OK

VMs made, partially configured and distributed to vCenter pod folders. Students need to use the instructions in this document to customize the VMs in their assigned pod.

To Do List

1. pfSense (2.3.1, 64 bit) - configure IPv6
2. Kali (2016.1, 64 bit) - start sshd on restart, permanent nameserver config
3. Windows XP (SP2, 32 bit) - uncheck hide suffixes

Admonition

Unauthorized hacking is a crime.

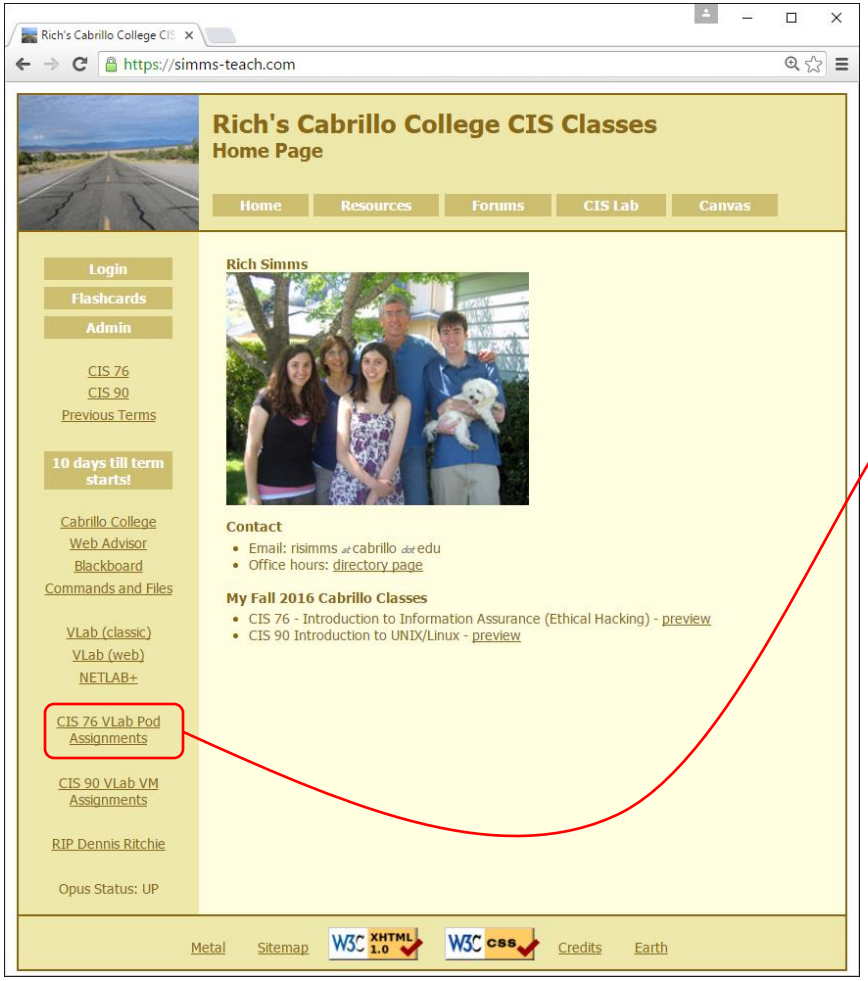
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

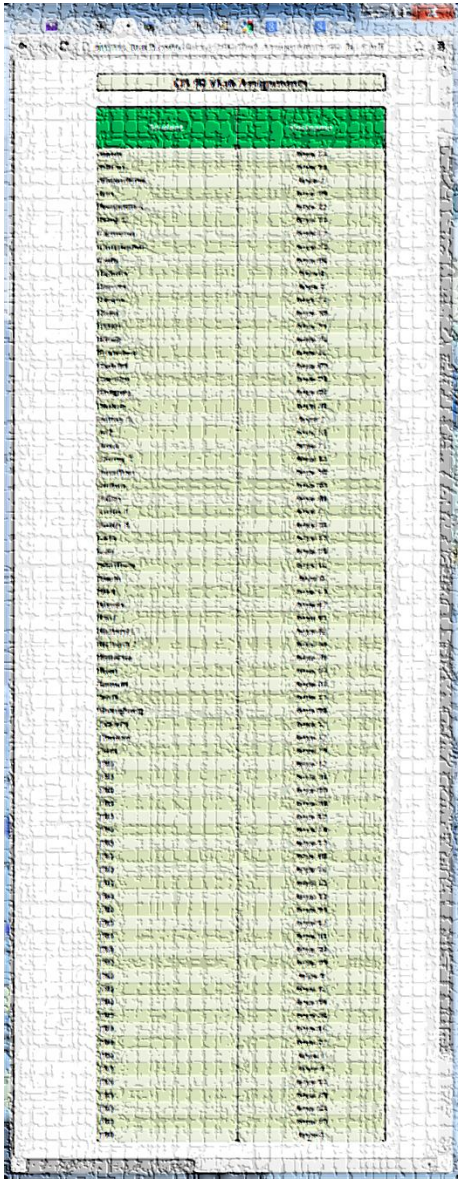
Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

VLab Pod Setup

CIS 76 - VLab Pod Setup

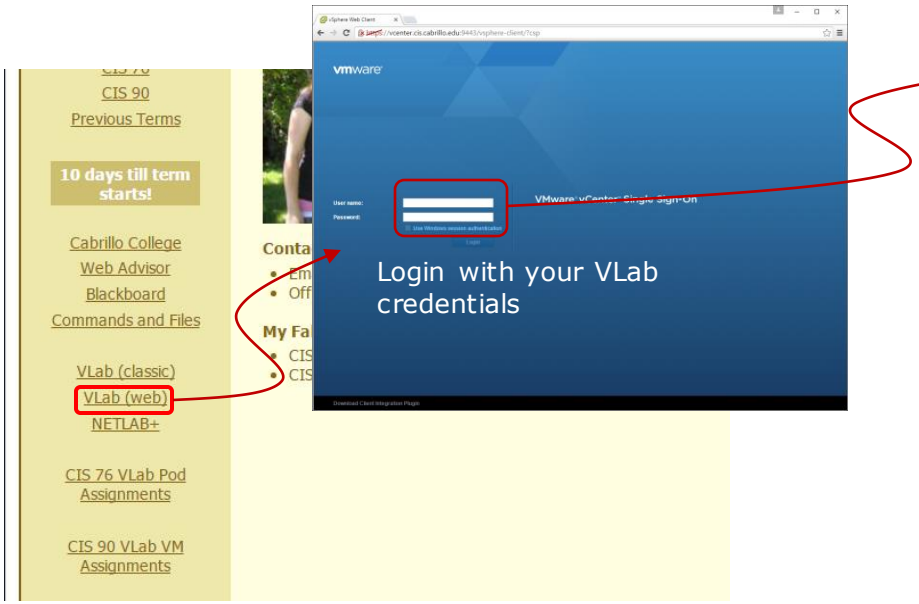
http://simms-teach.com/



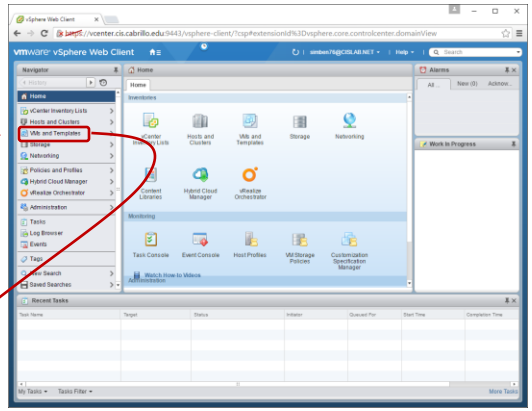


To see which pod is yours use the link on the class website

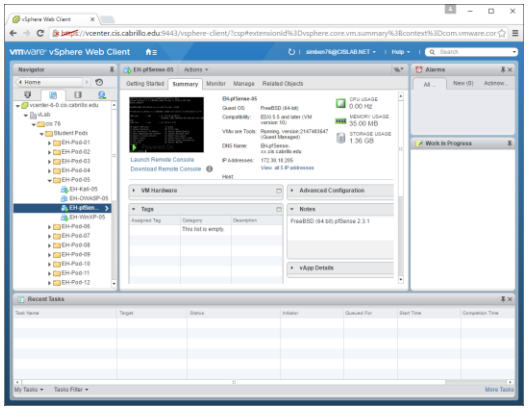
Accessing VLab
(vSphere Web Client via HTTPS)



http://simms-teach.com/



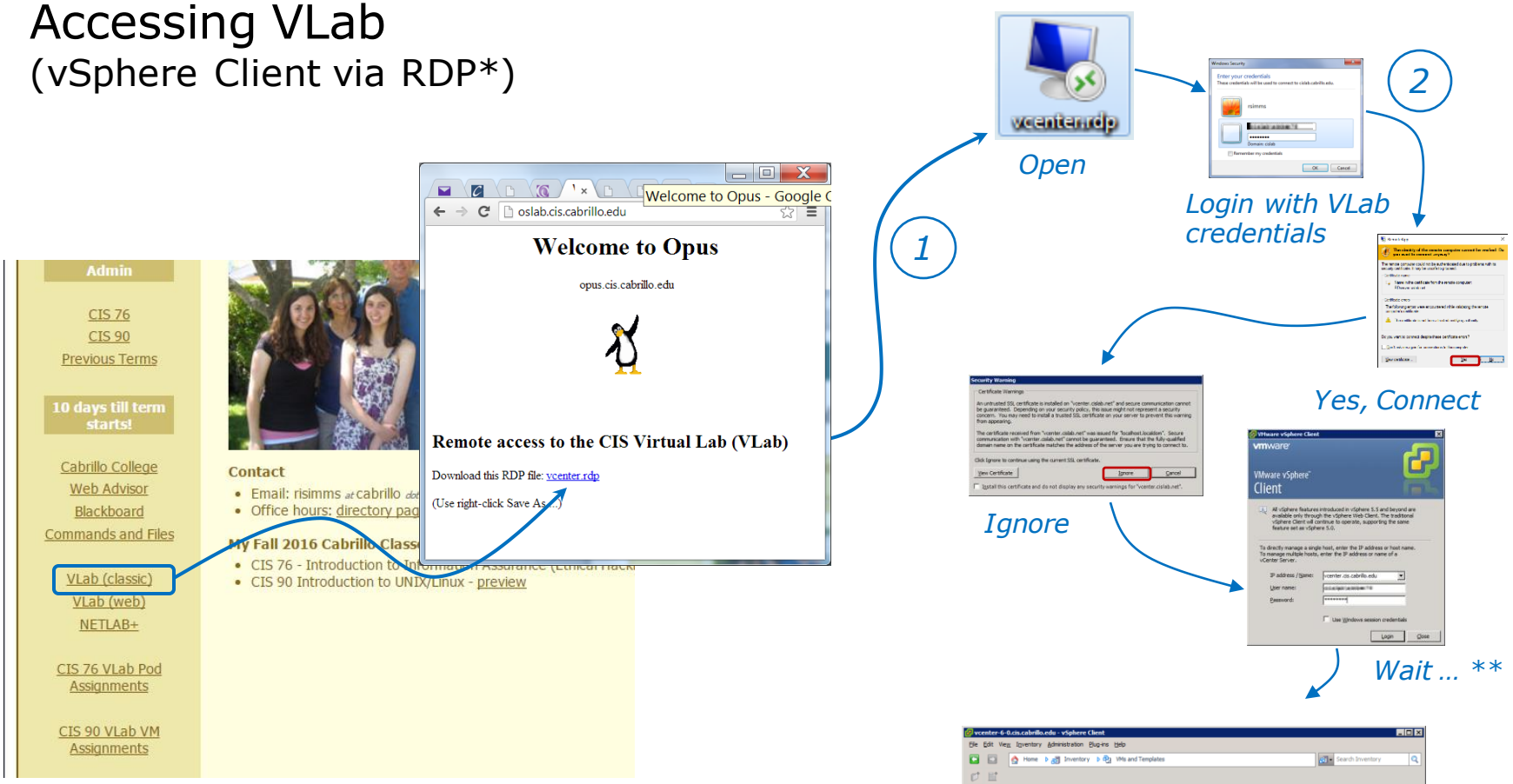
Select VM and Templates

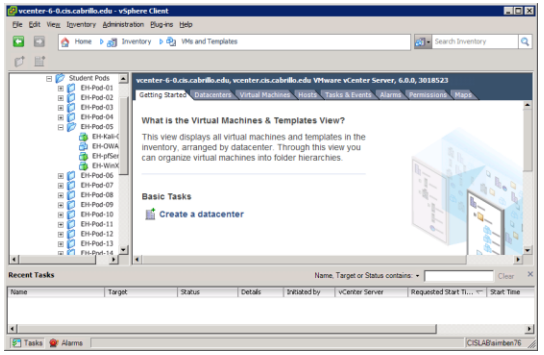


Expand containers and locate your pod VMs

The Web Client is simpler to access but the console views can have mouse selection issues on GUIs. Command line use works fine though.

Accessing VLab
(vSphere Client via RDP*)





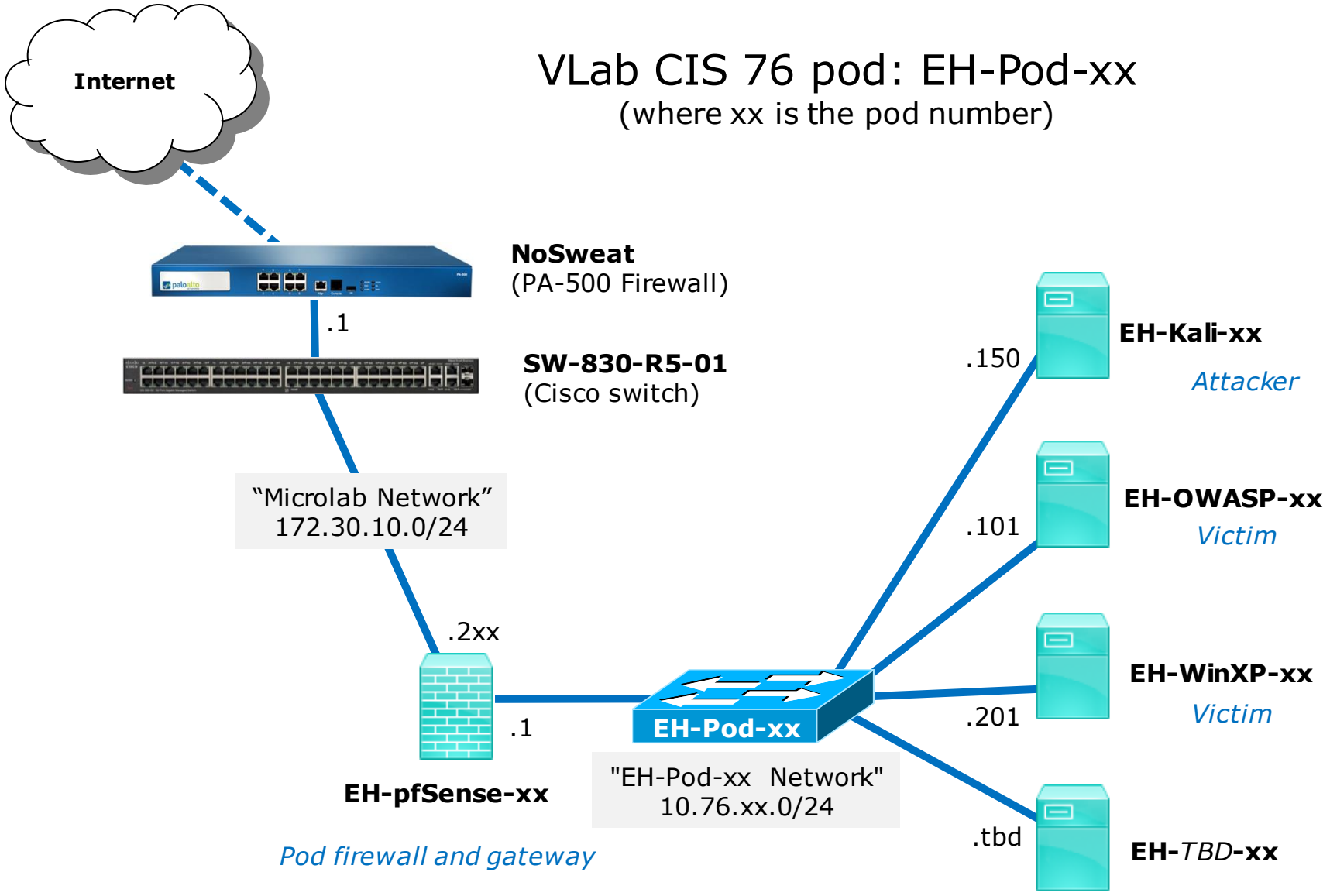
VMs and Templates view

*Mac users will need to install an RDP app like the Microsoft Remote Desktop app.

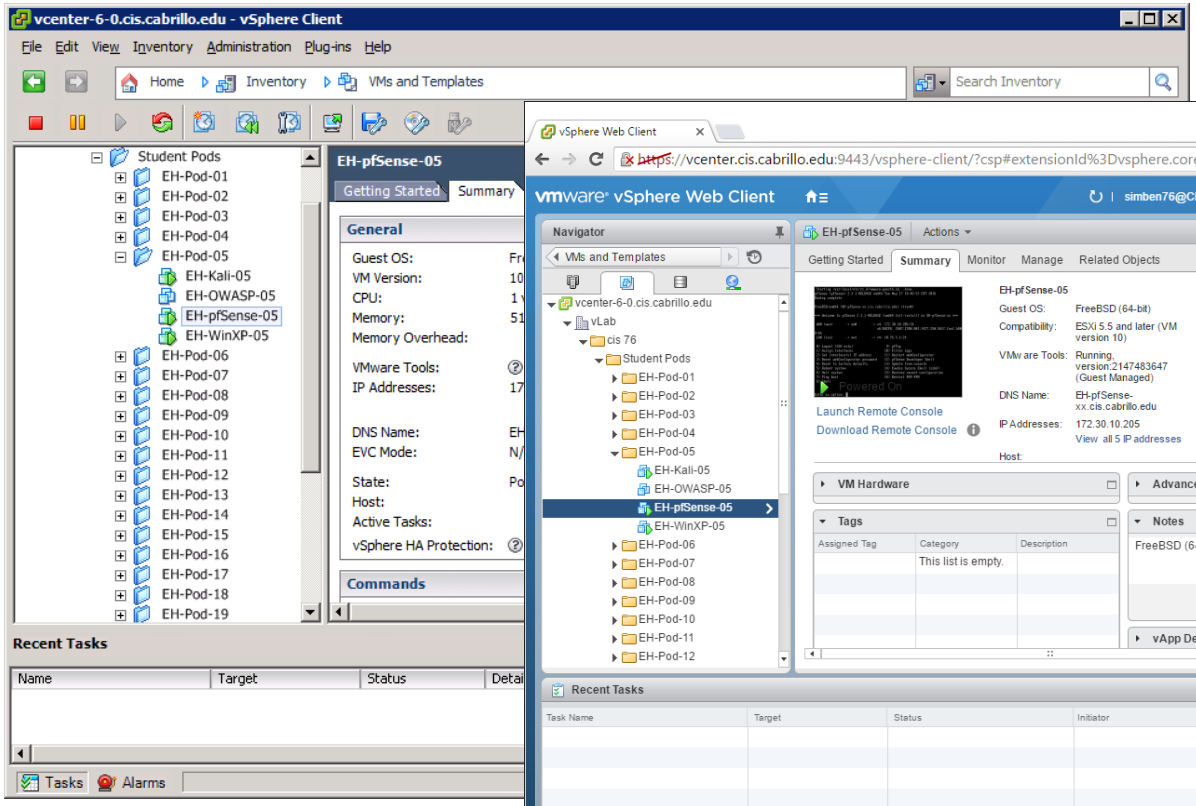
**Troubleshooting: If you get "Windows Credentials cannot be used to log into this server." then re-enter your credentials and try again with the "Use Windows session credentials option unchecked".

VLab CIS 76 pod: EH-Pod-xx

(where xx is the pod number)



CIS VLab (Virtual Lab) Student Pods



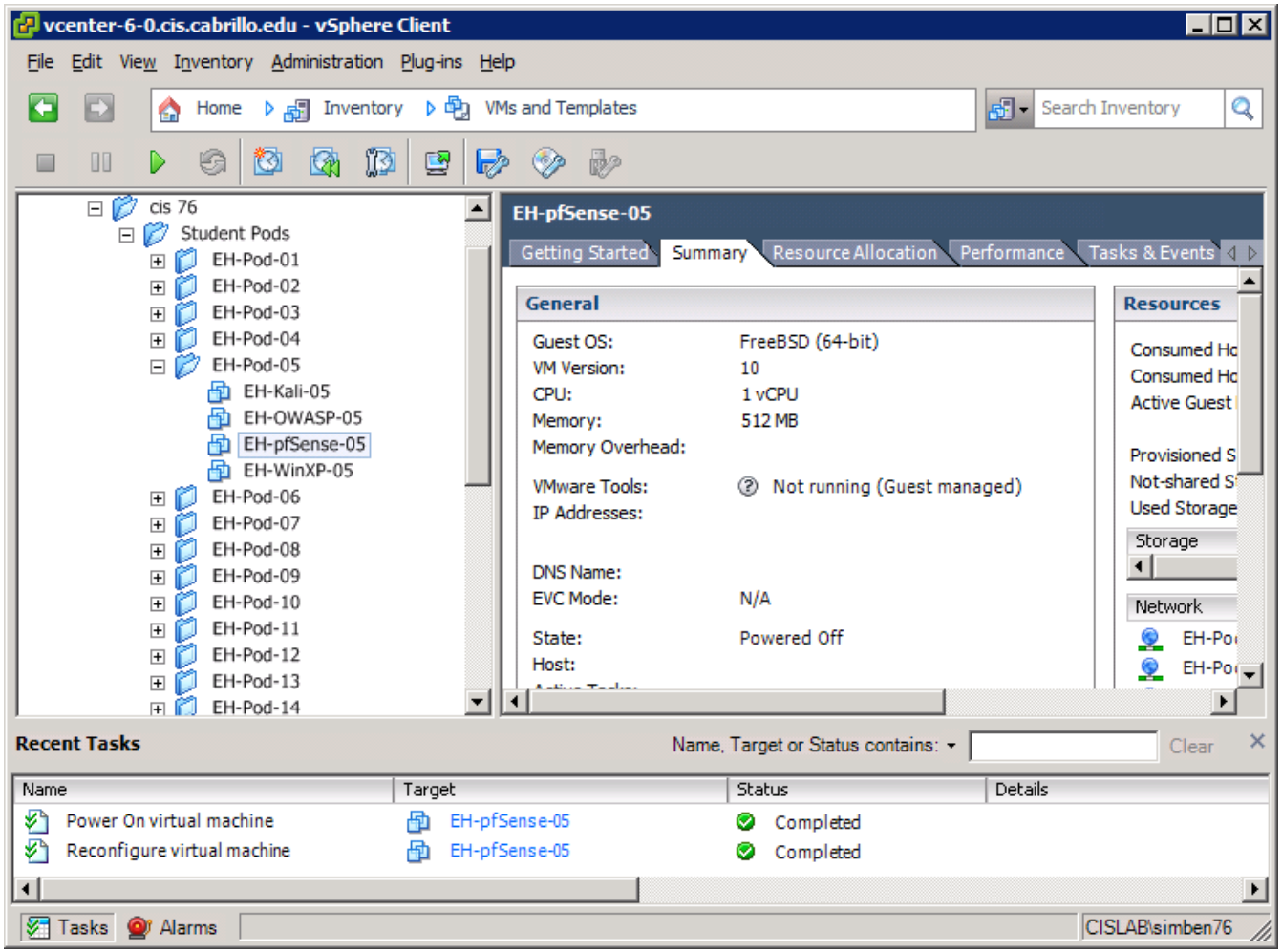
vSphere Client

vSphere Web Client

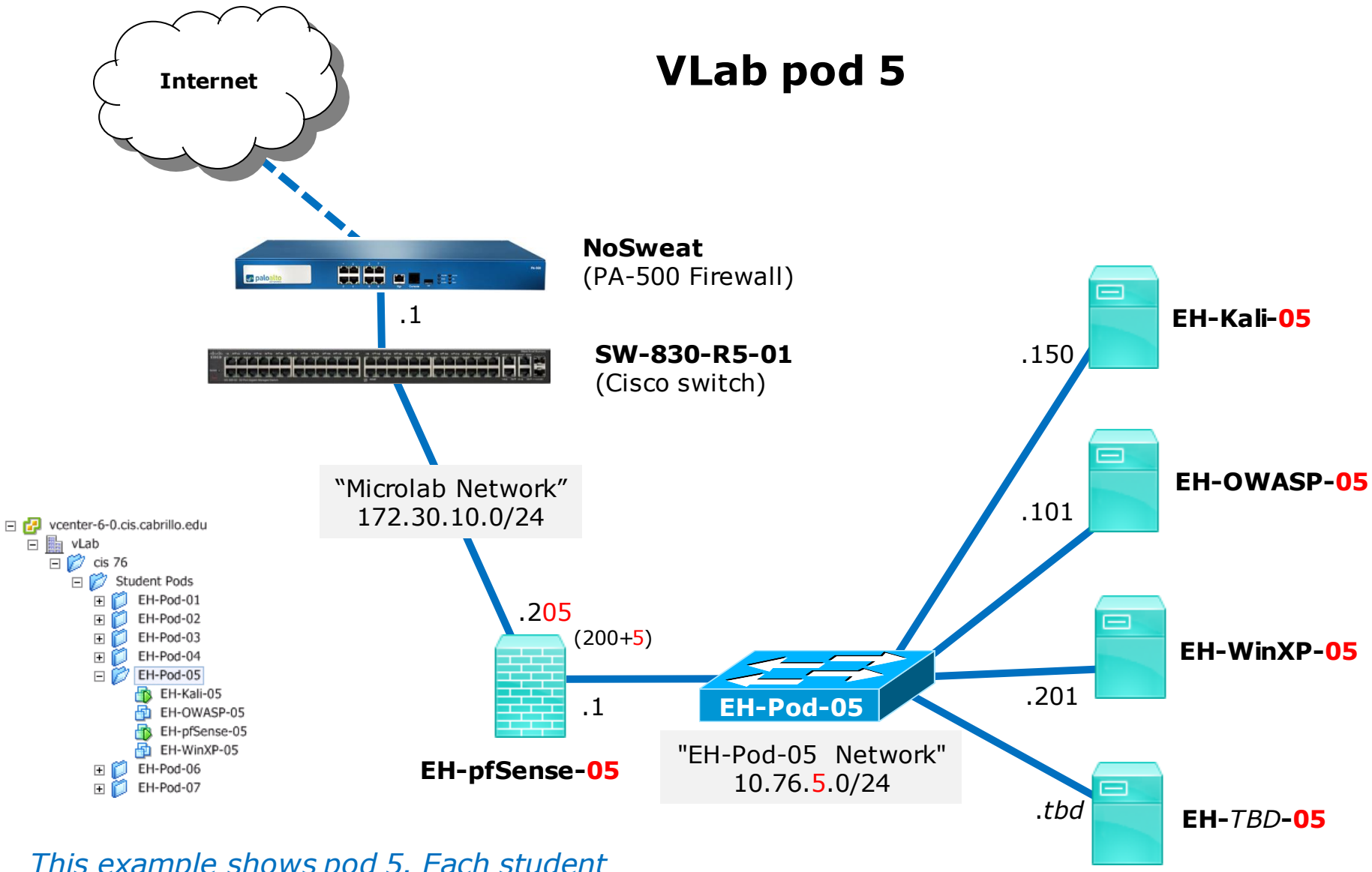
Students can use either vSphere Client or vSphere Web Client

pfSense VM Config

CIS VLab (Virtual Lab) Student Pods

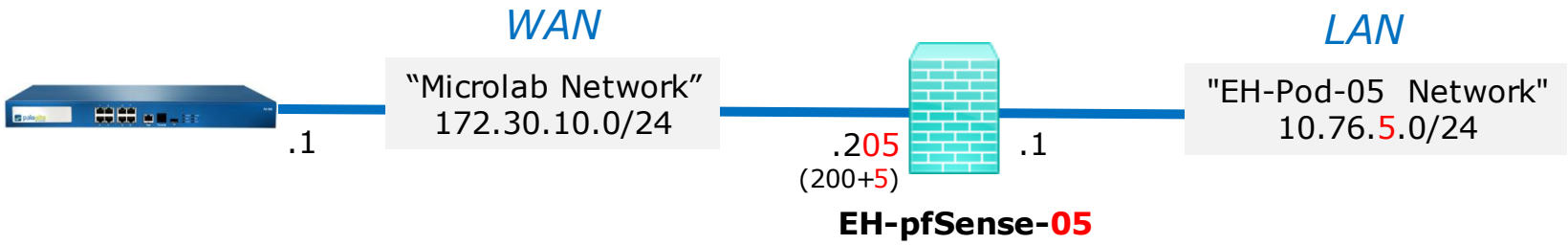


This example shows the pfSense VM in pod 5. Each student should only use the pod assigned to them.



This example shows pod 5. Each student should only use the pod assigned to them.

Example: Configuring the EH-pfSense VM in EH-Pod-05

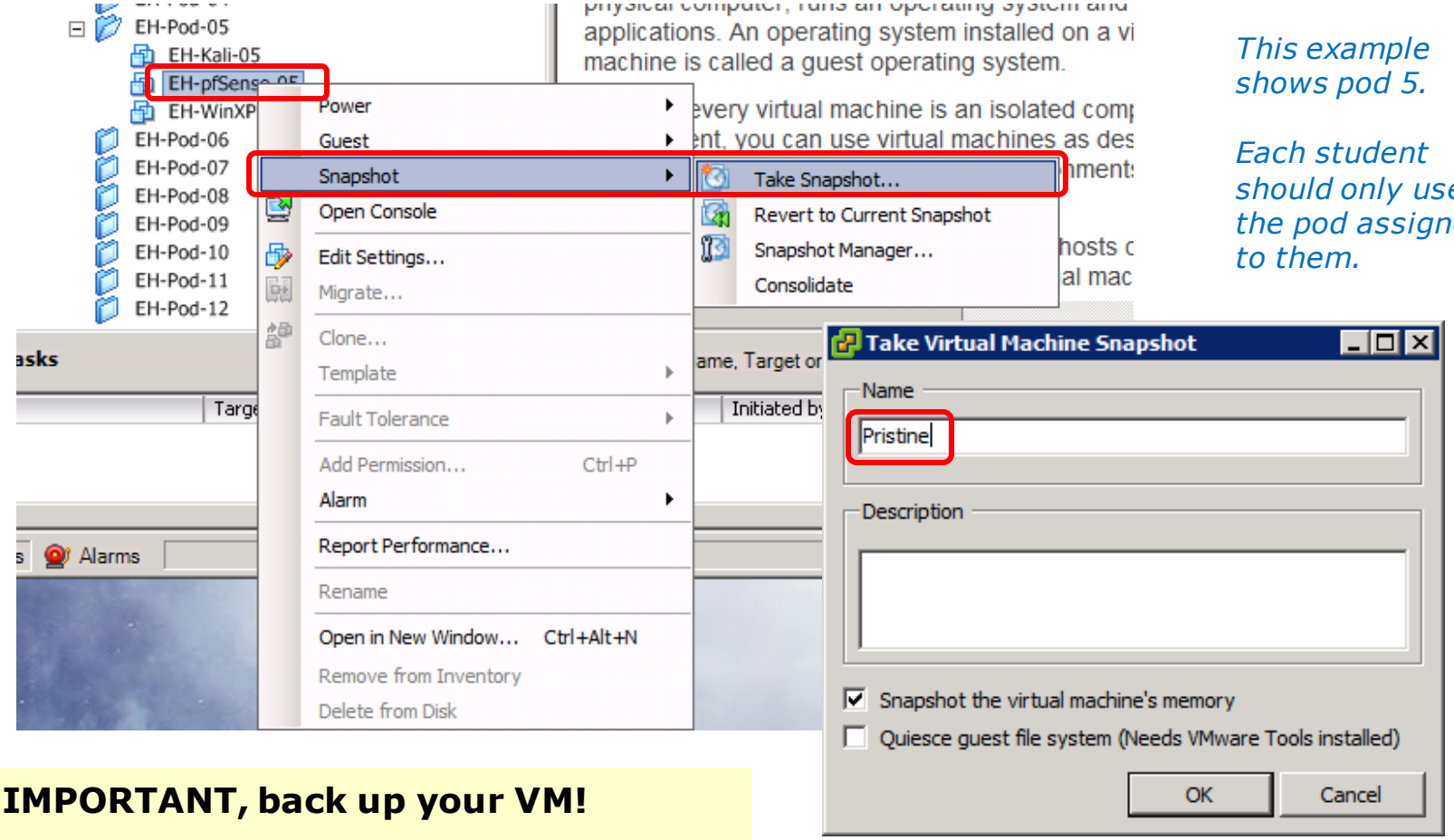


This example shows pod 5.

Each student should only use the pod assigned to them.

pfSense VM	Pod 5 settings
VM Network Adapter 1	uLab Net
VM Network Adapter 2	EH-Pod-05 Net
Hostname	EH-pfSense-05
WAN IPv4	172.30.10.205
WAN subnet bits	24
WAN upstream gateway	172.30.10.1
WAN IPv6	DHCP6
LAN webConfigurator	Use HTTPS
LAN IPv4	10.76.5.1
LAN subnet bits	24
LAN DHCP service	disabled
LAN webConfigurator	Use HTTPS

Example: Configuring the EH-pfSense VM in EH-Pod-05



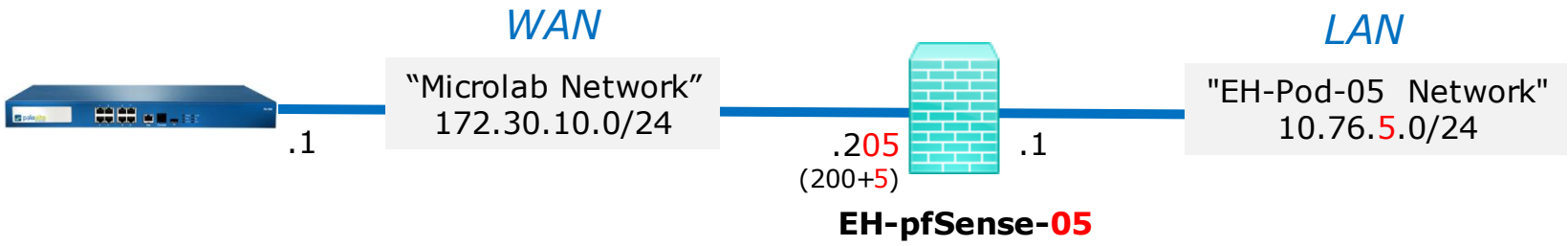
This example shows pod 5.

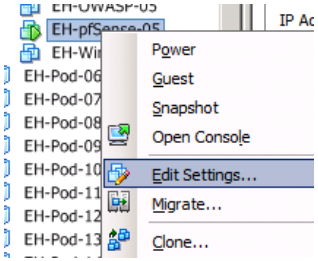
Each student should only use the pod assigned to them.

IMPORTANT, back up your VM!

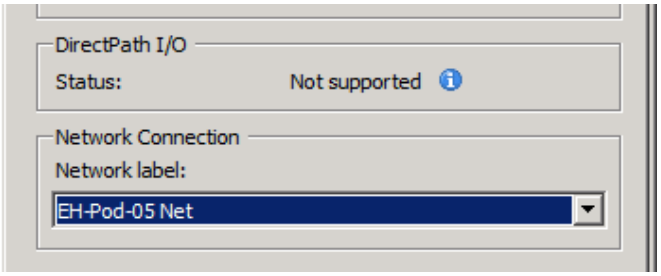
1) Make a backup snapshot of your pfSense VM named "Pristine".

Example: Configuring the EH-pfSense VM in EH-Pod-05





This example shows pod 5. Each student should only use the pod assigned to them.



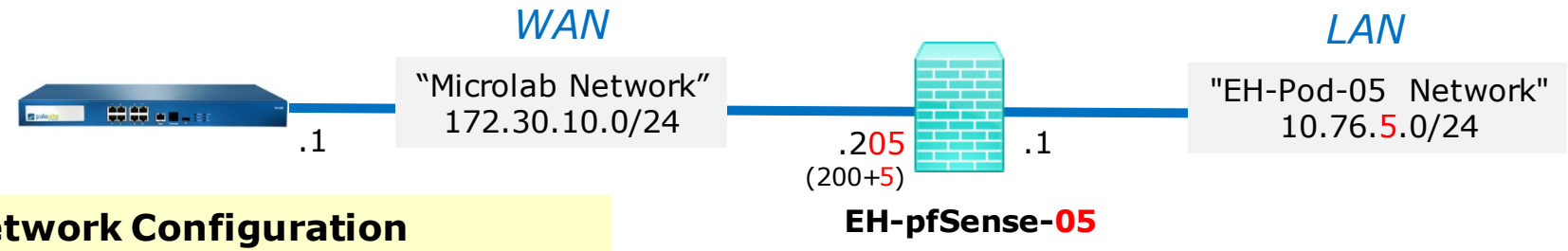
Network Cabling

1) Edit the settings of your pfSense VM.

2) Network Adapter 1 should be connected to the "uLab Net" (Microlab network).

3) Network Adapter 2 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

Example: Configuring the EH-pfSense VM in EH-Pod-05



Network Configuration

1) Figure out the IPv4 addresses for the WAN and LAN interfaces:

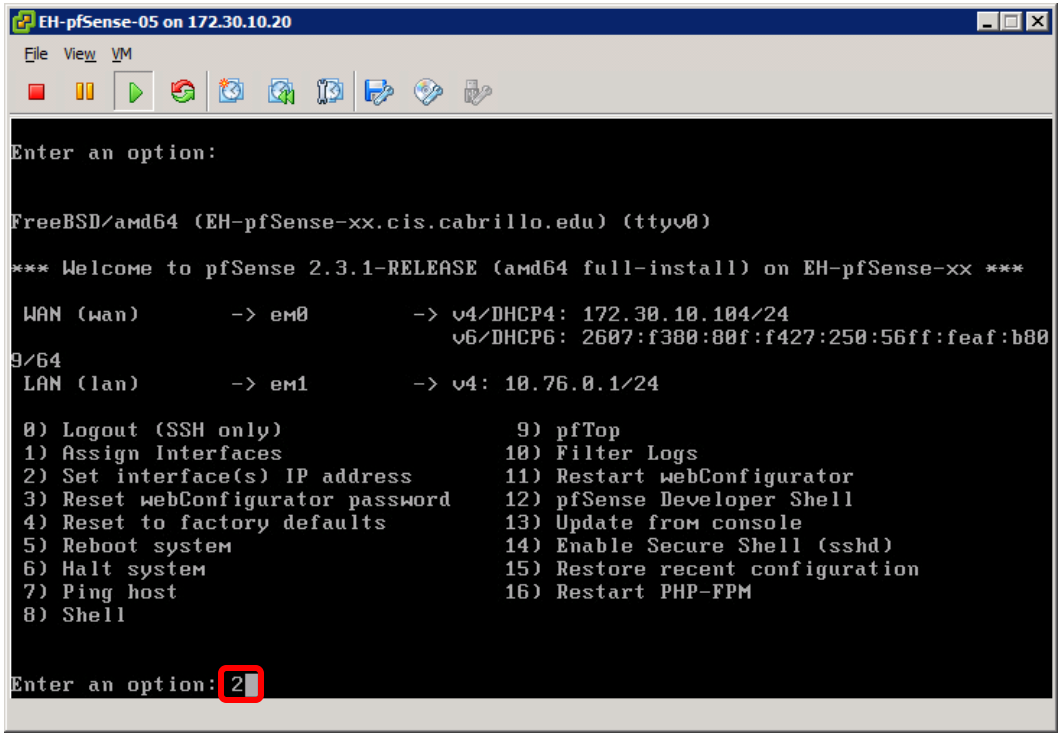
WAN: 172.30.10.xxx, where xxx is 200+your pod number.

LAN: 10.76.xx.1, where xx is your pod number.

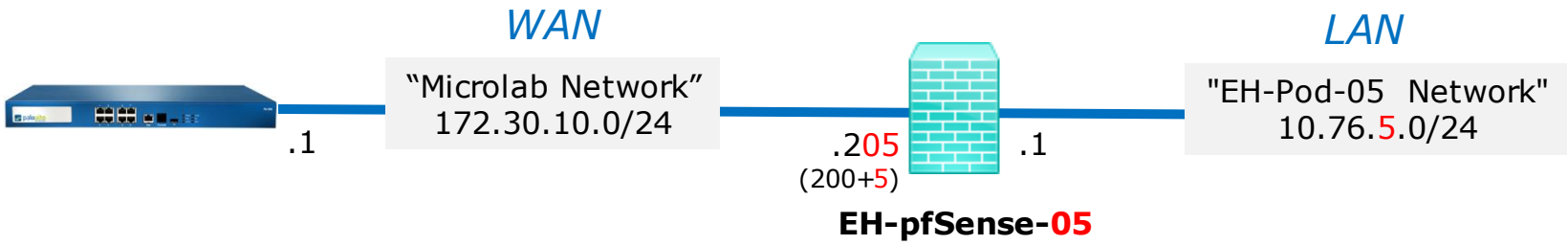
2) Power up the VM and open a console.

3) Wait till you see the menu options (0-16).

4) Select Option 2 to set IP addresses on the interfaces.



Example: Configuring the EH-pfSense VM in EH-Pod-05



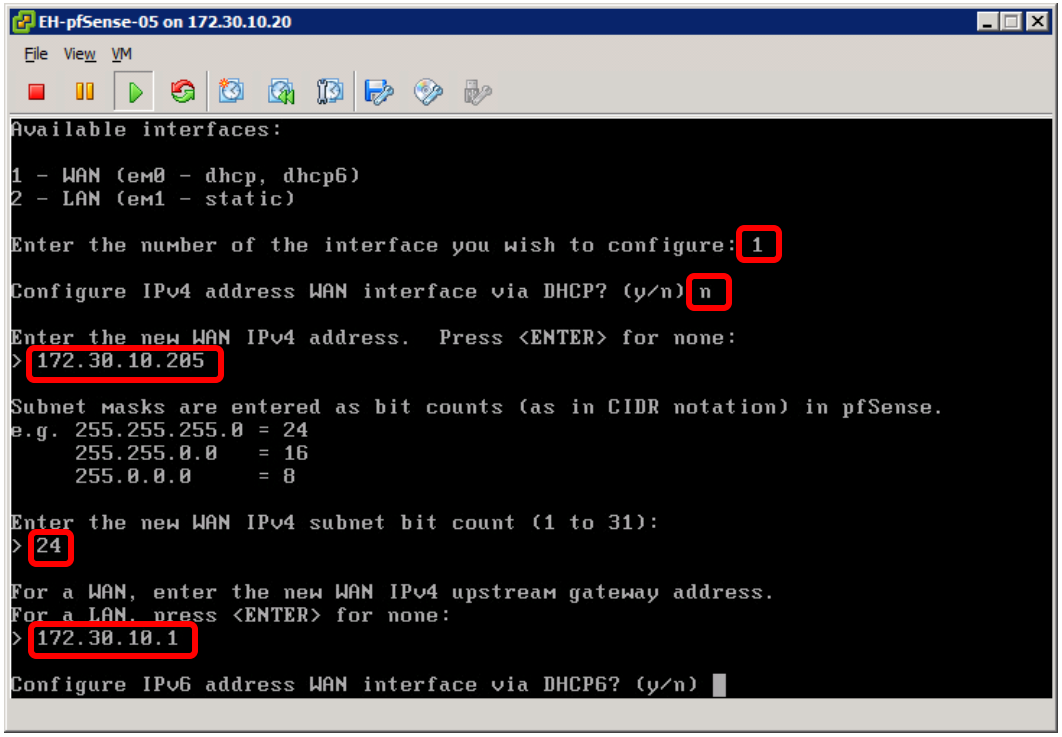
5) Select Option 1 to configure the WAN interface.

6) We are going to set a static IP address so select "n" when asked to use DHCP.

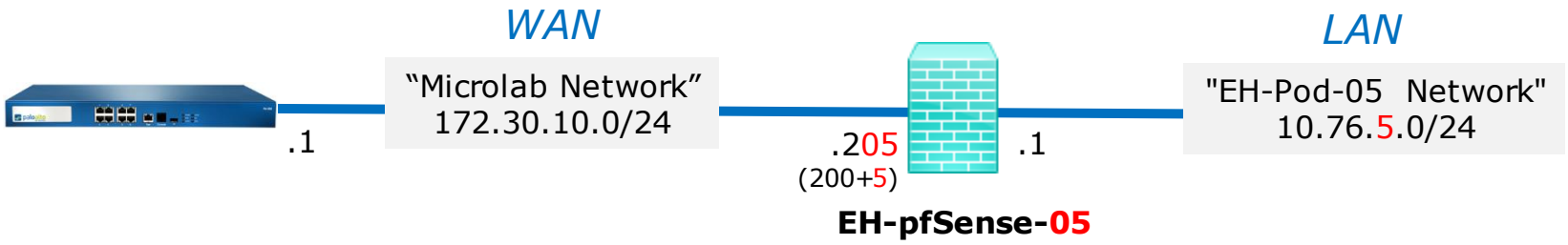
7) Enter your outside WAN IP address. Add your pod number to 200 to determine the 4th octet. For Pod 5 the WAP IP address will be 172.30.10.205.

8) Select 24 bits for the subnet mask.

9) Set the upstream gateway to 172.30.10.1.



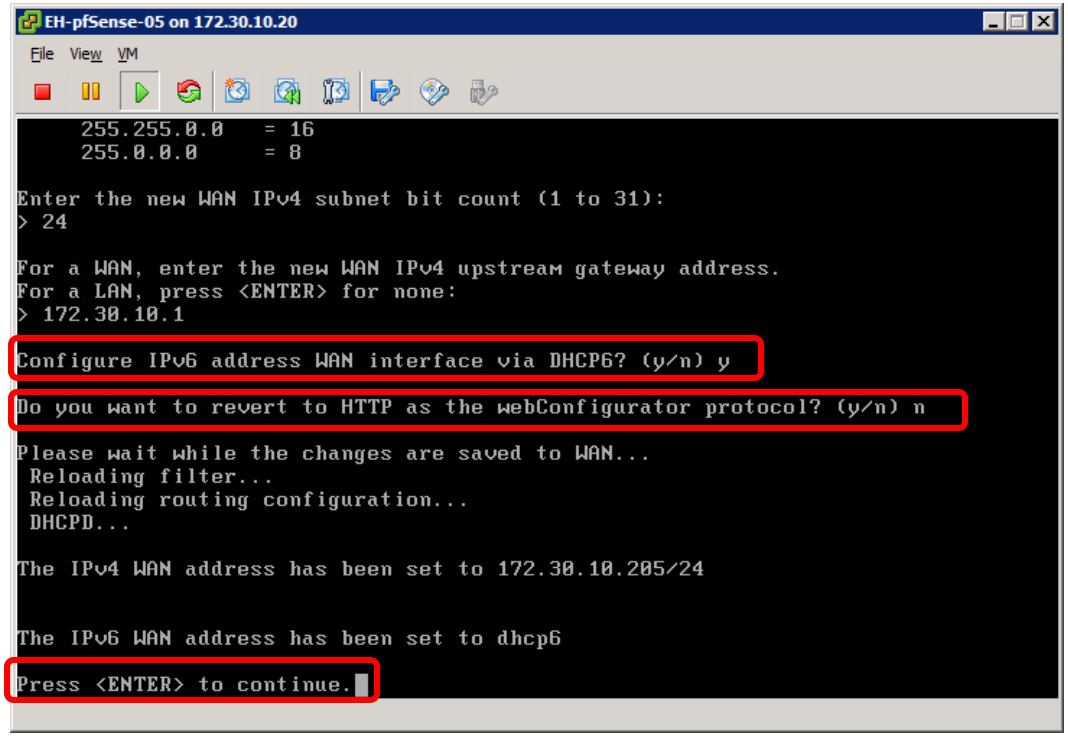
Example: Configuring the EH-pfSense VM in EH-Pod-05



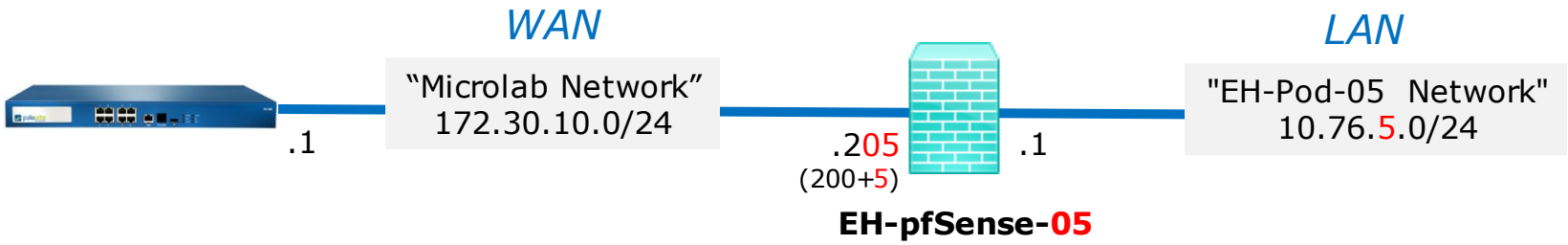
10) Enter "y" to use the DHVP6 for the IPv6 address.

11) Enter "n" to not revert to HTTP as the webConfigurator protocol.

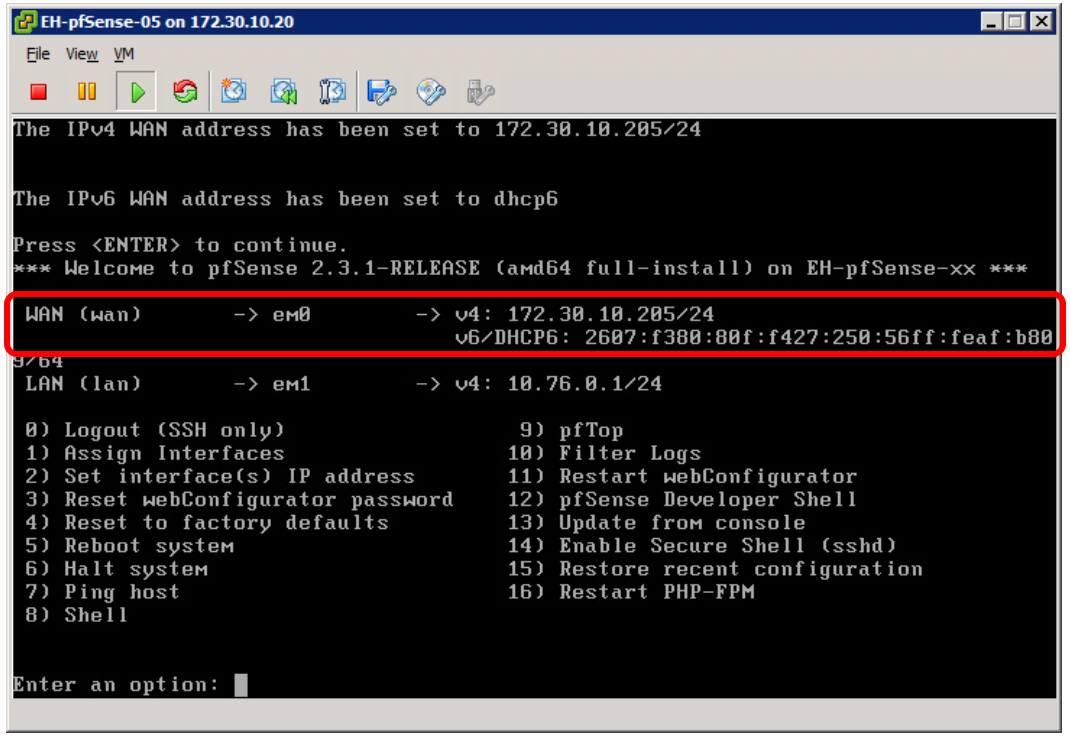
12) Press <ENTER> to continue.



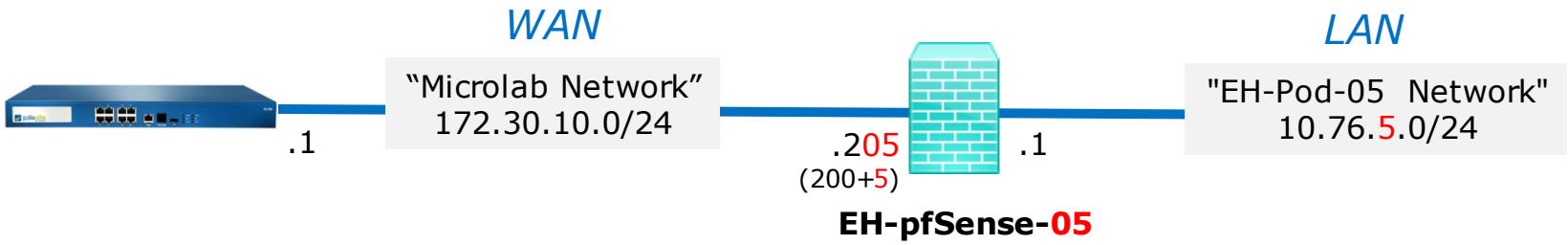
Example: Configuring the EH-pfSense VM in EH-Pod-05



13) Verify the WAN interface was setup correctly.



Example: Configuring the EH-pfSense VM in EH-Pod-05



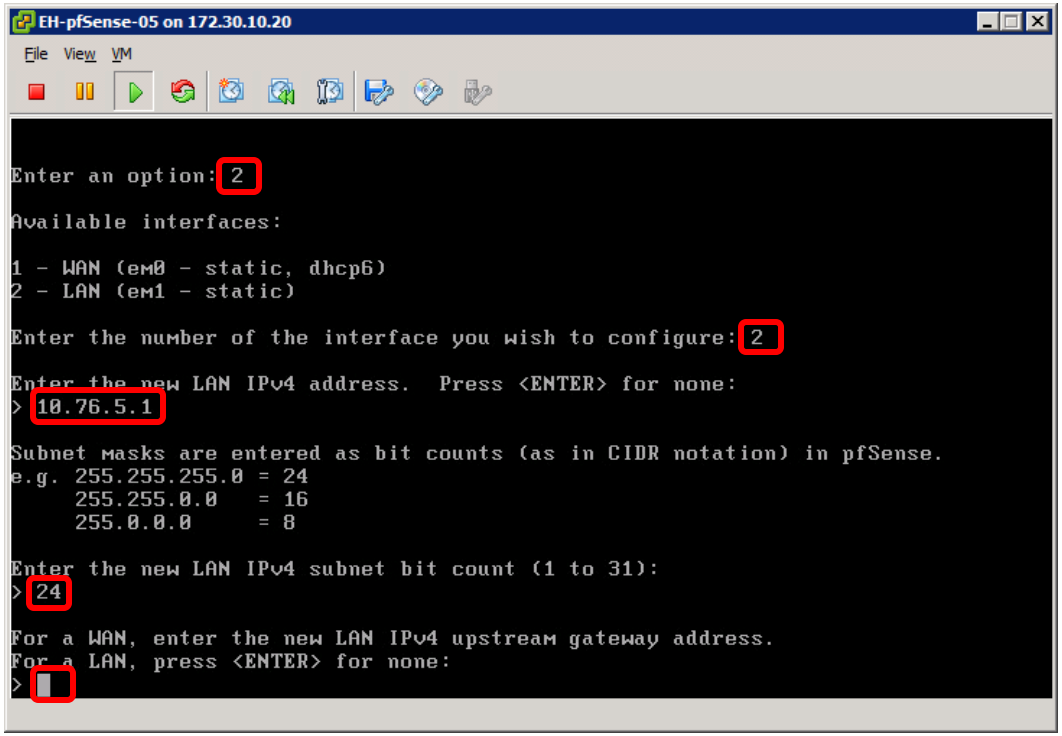
14) Select option 2 again on the main menu to set an IP address on an interface.

15) Select option 2 for LAN.

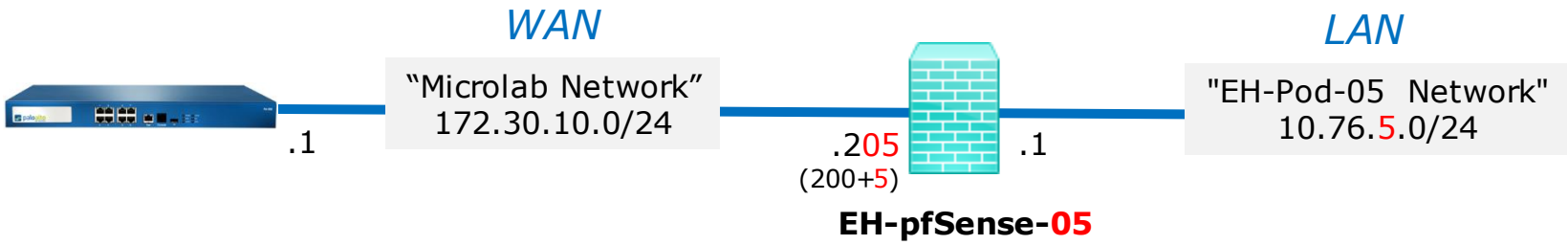
16) Set the IP address. Make the third octet your pod number. For example the Pod 5 IP address is 10.76.5.1.

17) Select 24 bits for the subnet mask.

18) Press <ENTER> for none since we don't need to set the upstream gateway again.



Example: Configuring the EH-pfSense VM in EH-Pod-05

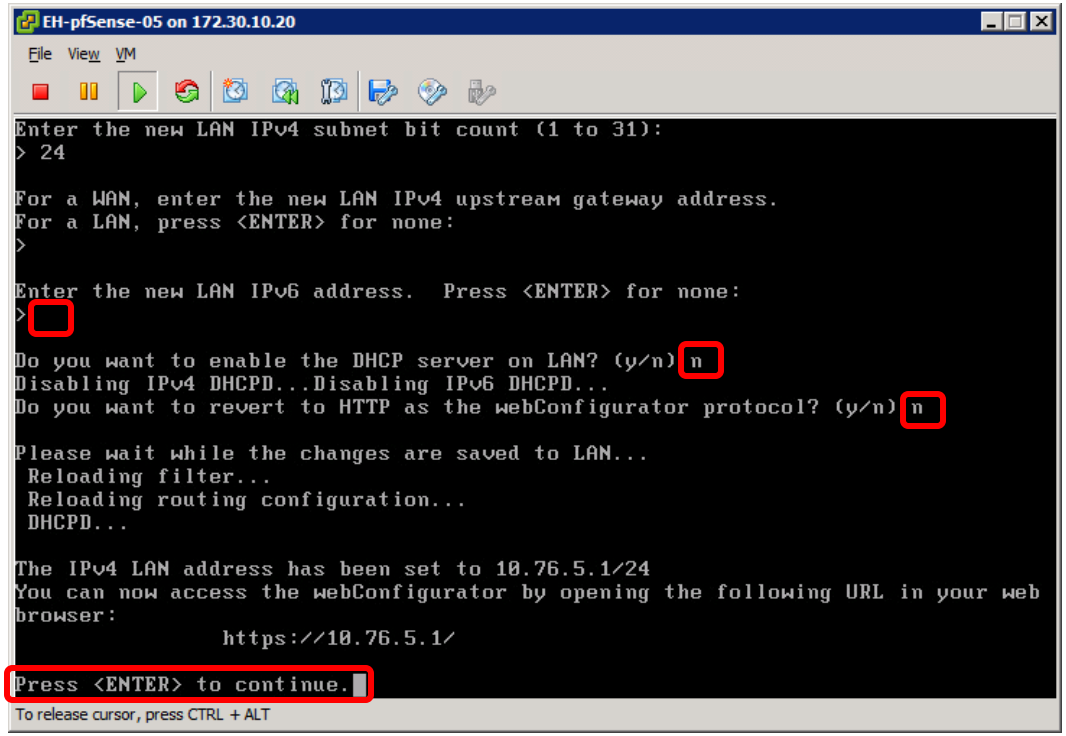


19) Press <ENTER> for none when prompted for the IPv6 address.

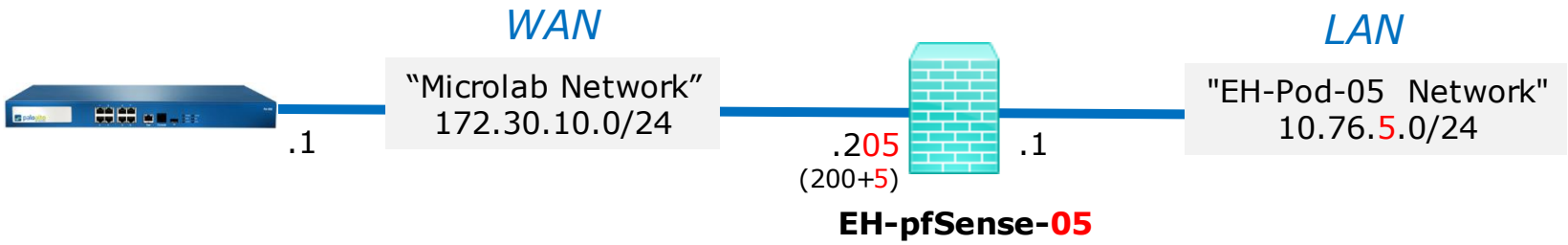
20) Enter "n" to not setup DHCP.

21) Enter "n" to not revert to HTTP for the webConfigurator. We will be using HTTPS.

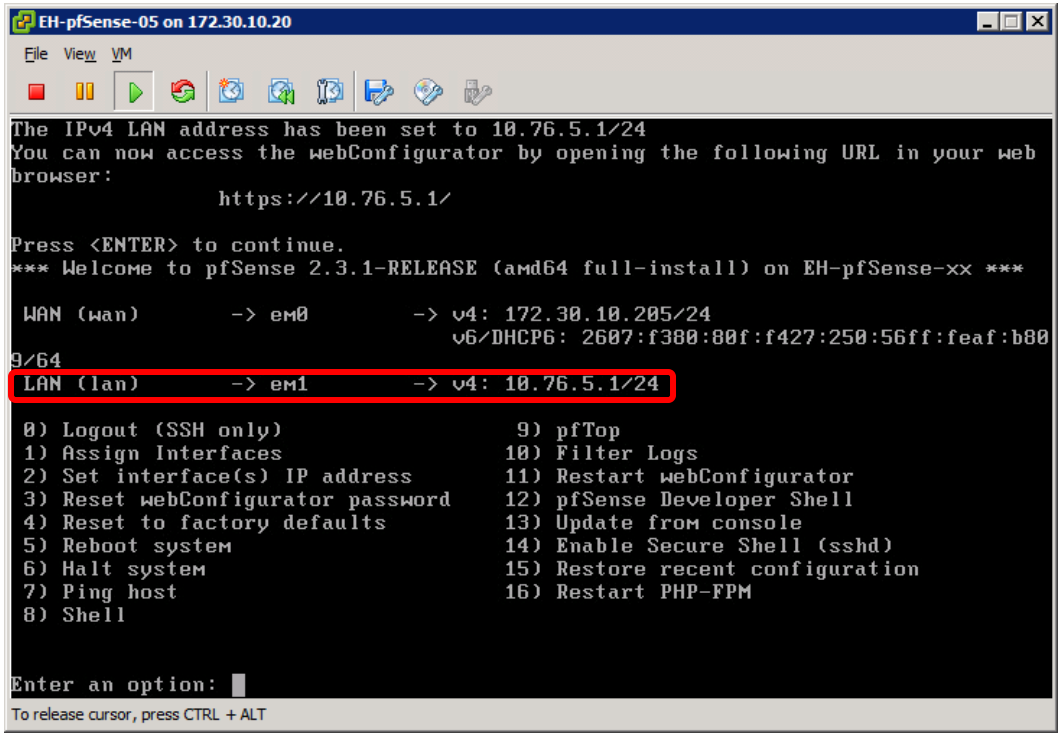
22) Press <ENTER> to continue.



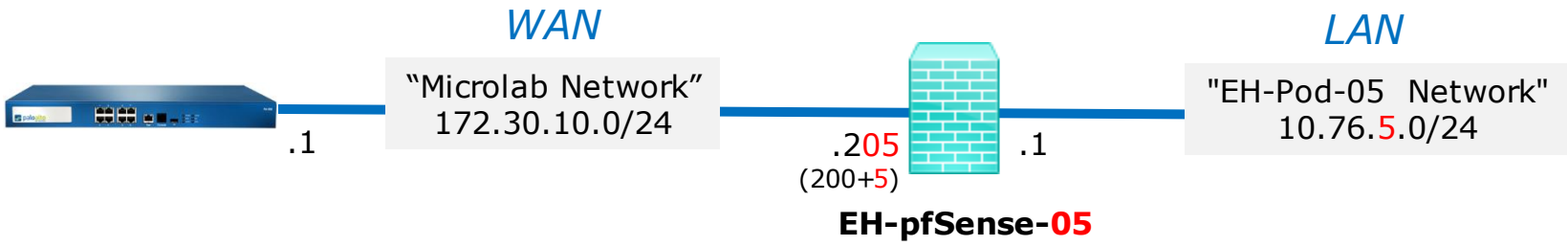
Example: Configuring the EH-pfSense VM in EH-Pod-05



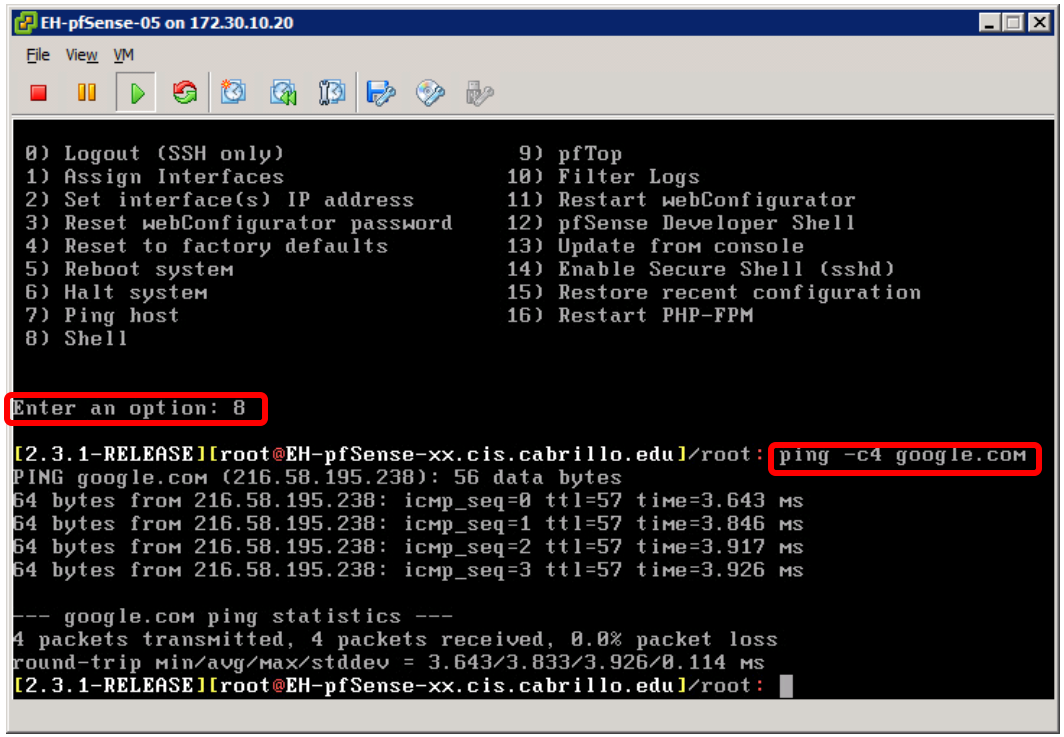
23) Verify the IP address on your LAN interface. The third octet should be your pod number.



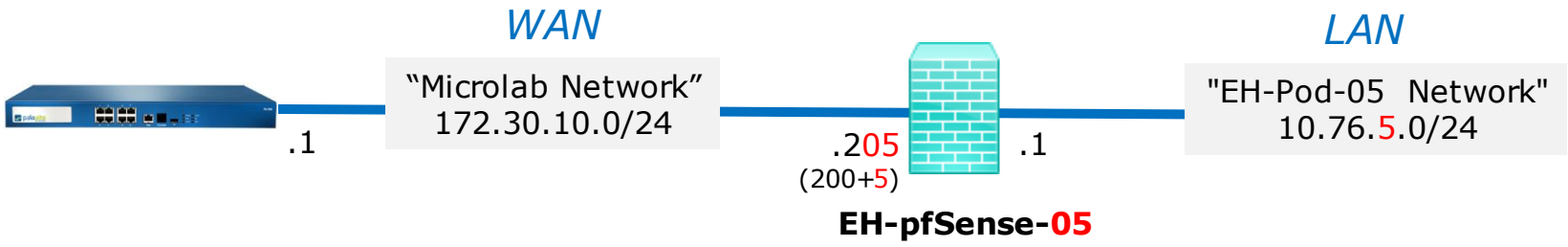
Example: Configuring the EH-pfSense VM in EH-Pod-05



24) Select option 8 to drop into the shell and verify you have Internet connectivity by pinging google.com

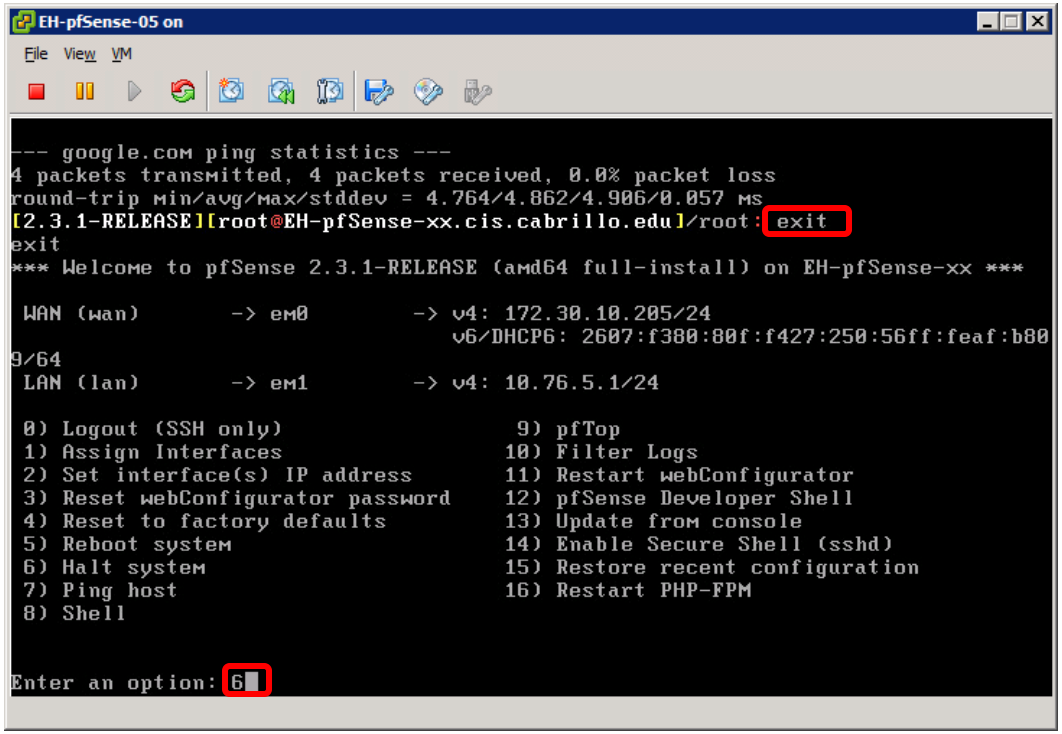


Example: Configuring the EH-pfSense VM in EH-Pod-05

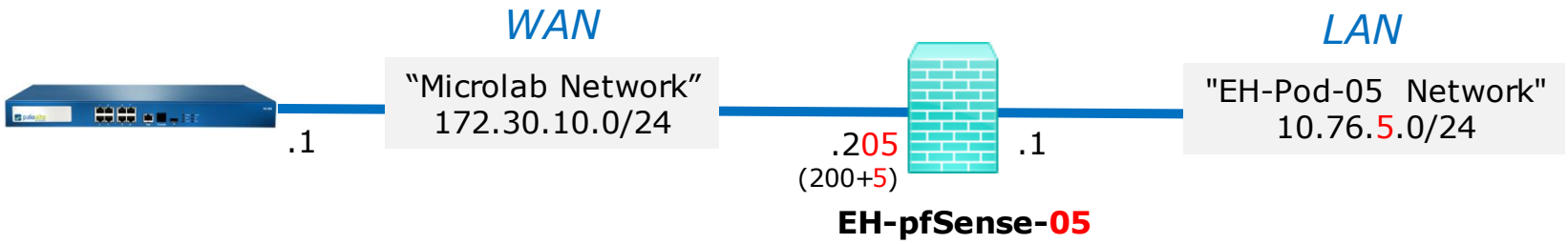


25) Type **exit** to return to the menu.

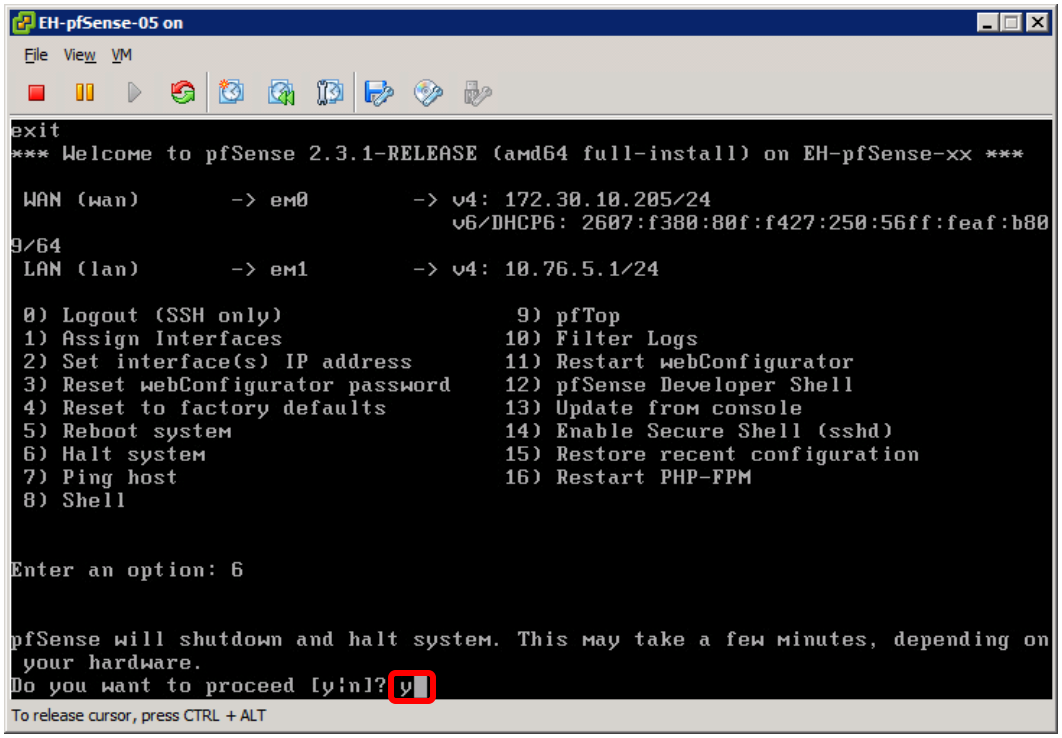
26) Select option 6 to shutdown the VM.



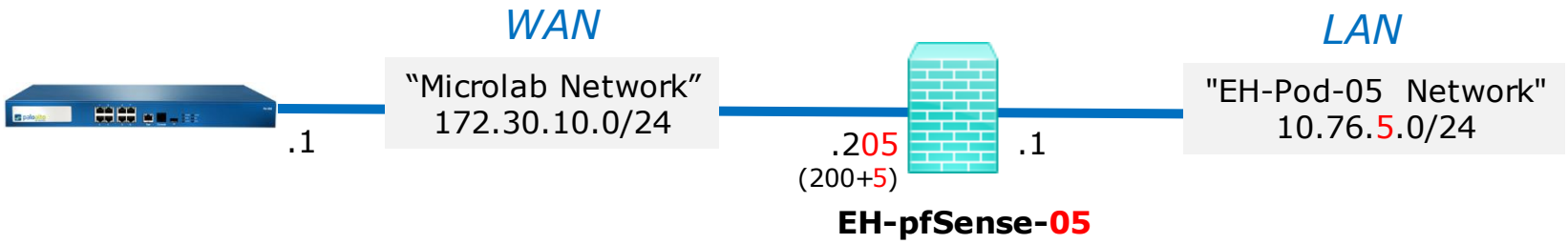
Example: Configuring the EH-pfSense VM in EH-Pod-05

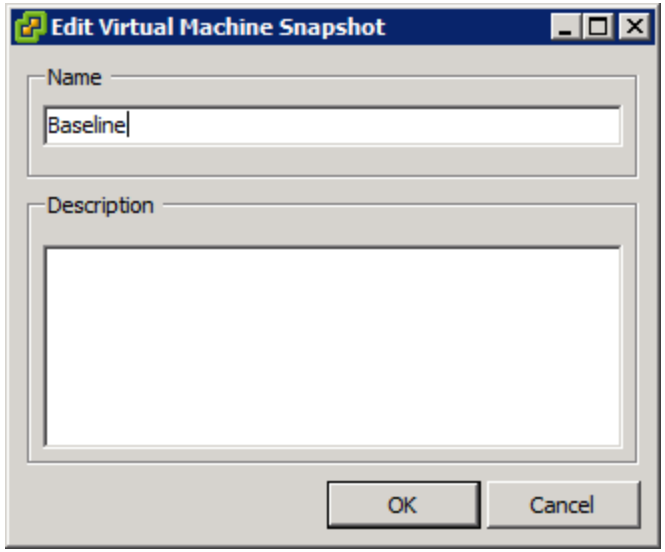


27) Type **y** to proceed.



Example: Configuring the EH-pfSense VM in EH-Pod-05

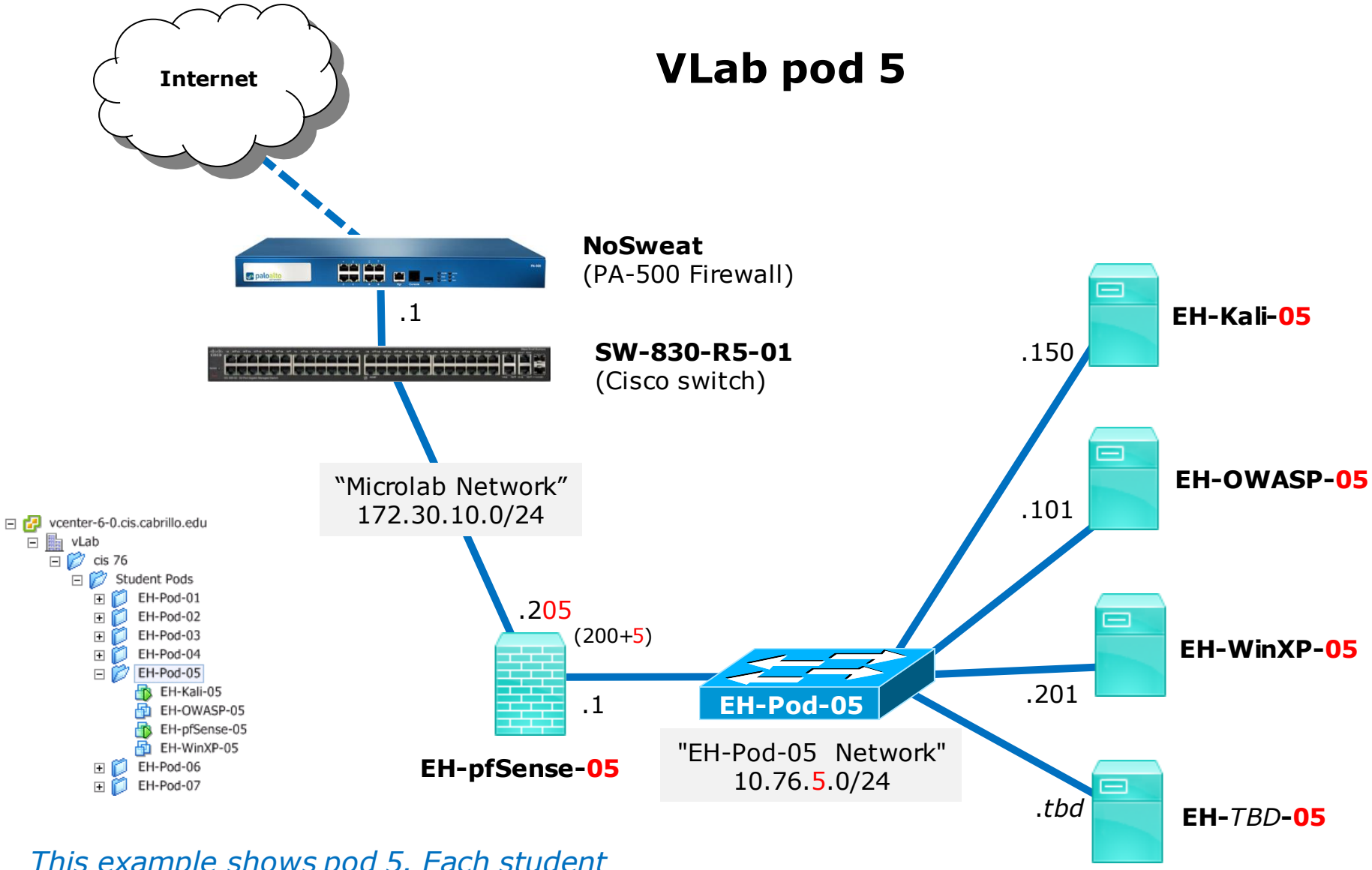




Save your work

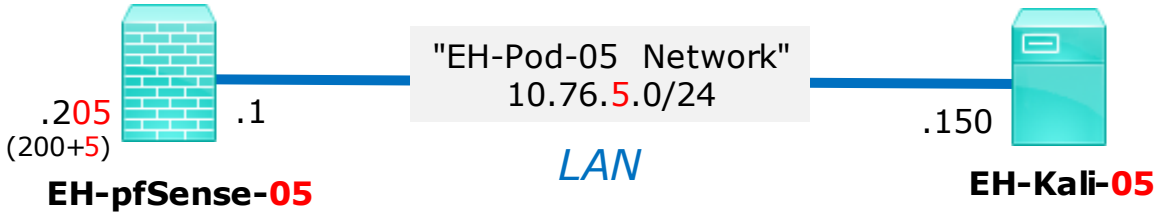
When the VM has shutdown make a second snapshot named "Baseline"

Kali VM Config



This example shows pod 5. Each student should only use the pod assigned to them.

Example: Configuring the EH-Kali VM in EH-Pod-05

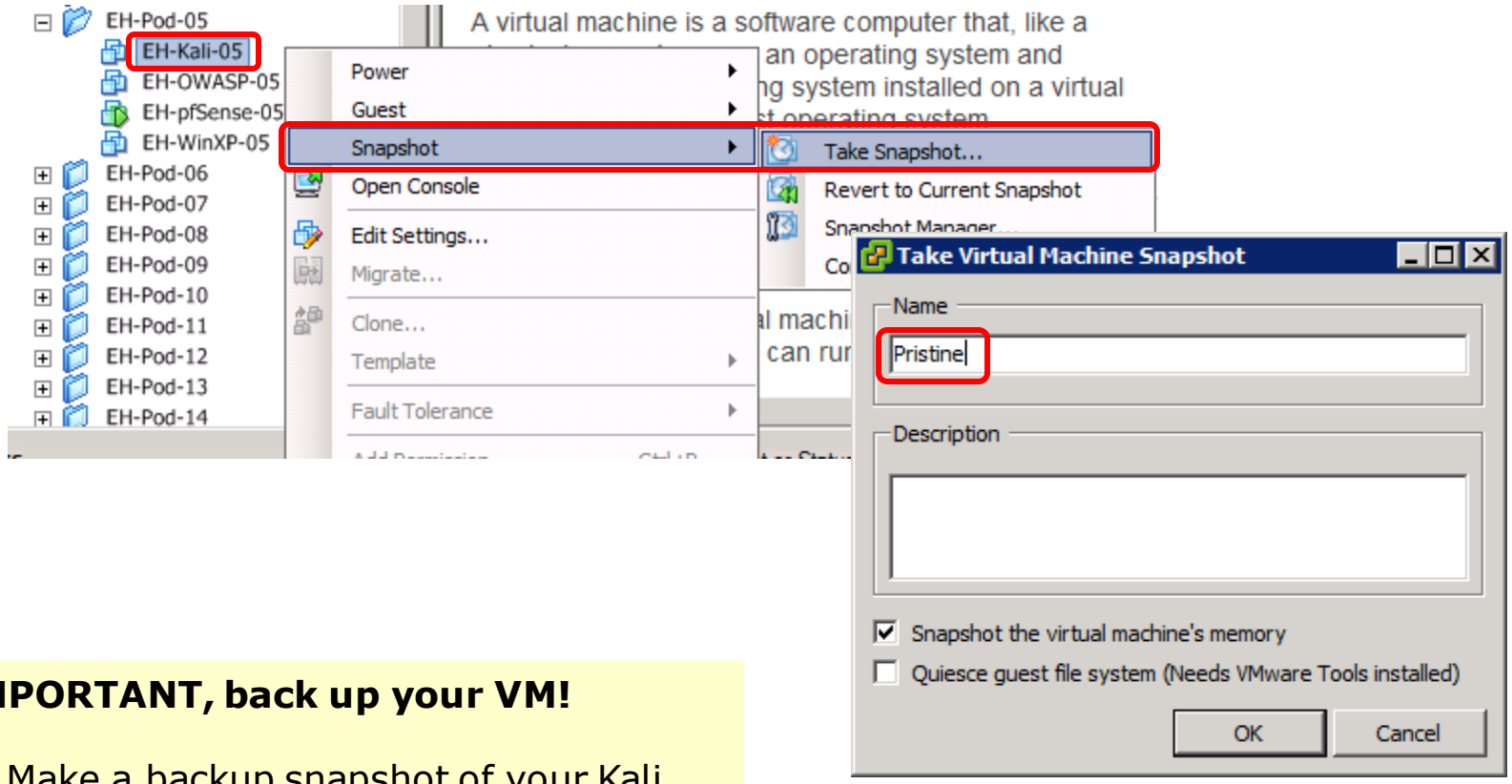


This example shows pod 5.

Each student should only use the pod assigned to them.

Kali VM	Pod 5 settings
VM Network Adapter 1	EH-Pod-05 Net
Hostname	EH-Kali-05
IPv4 address	10.76.5.150
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.5.1

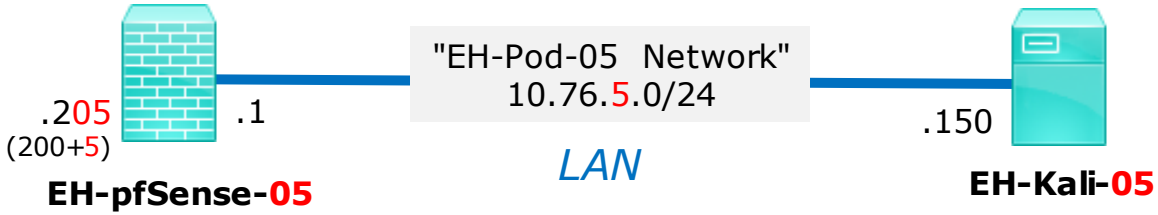
Example: Configuring the EH-Kali VM in EH-Pod-05

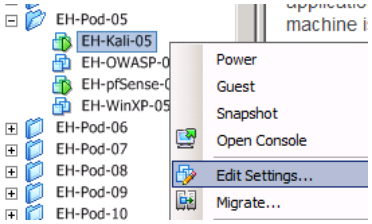


IMPORTANT, back up your VM!

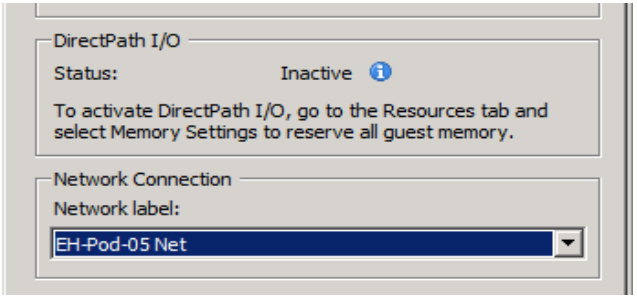
1) Make a backup snapshot of your Kali VM named "Pristine".

Example: Configuring the EH-Kali VM in EH-Pod-05





This example shows pod 5. Each student should only use the pod assigned to them.

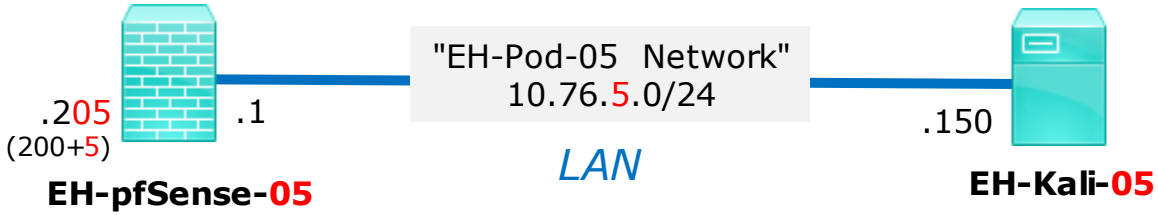


Network Cabling

1) Edit the settings of your Kali VM.

2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

Example: Configuring the EH-Kali VM in EH-Pod-05

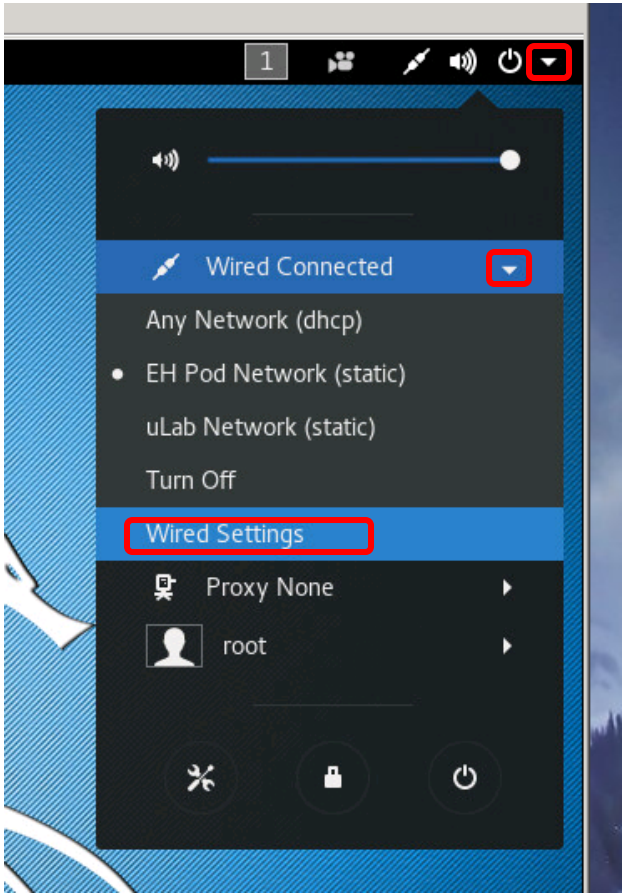


Network Configuration

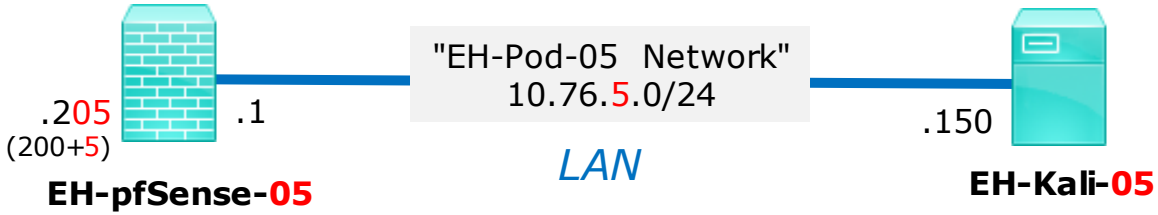
1) Power up the VM and open a console.

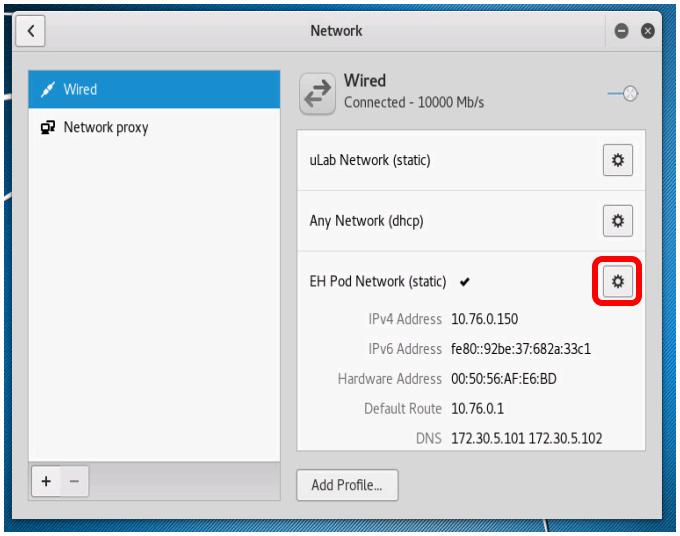
2) Login as the root user.

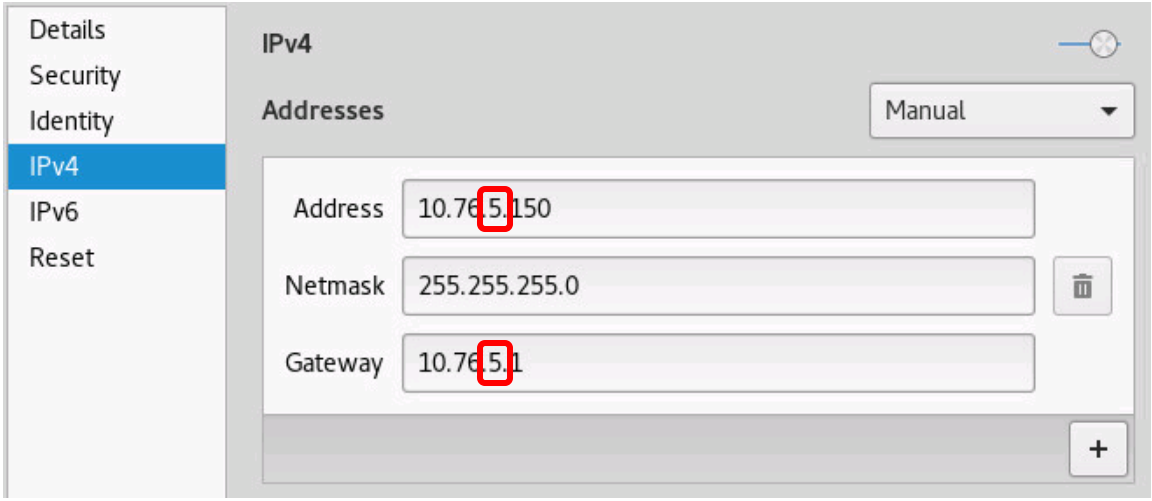
3) Select Wired Connected > Wire Settings using the pull down arrows.



Example: Configuring the EH-Kali VM in EH-Pod-05





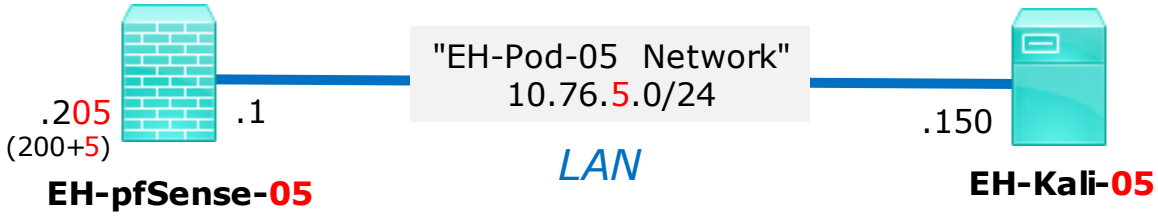


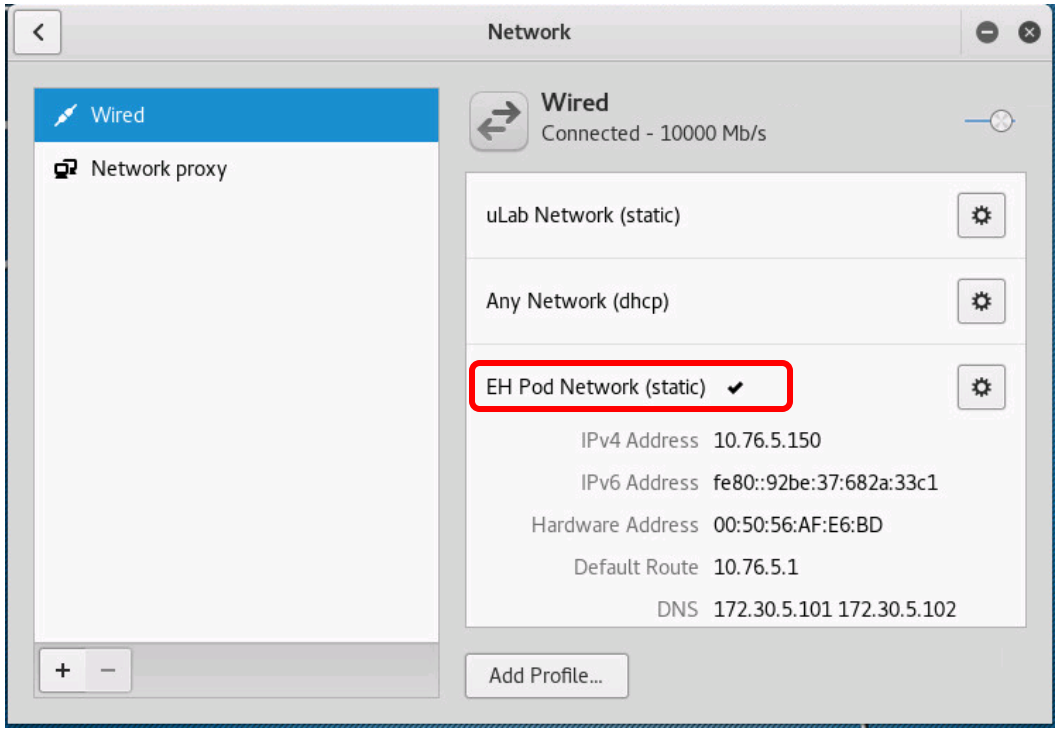
This example shows pod 5. Each student should only use the pod assigned to them.

4) Click the gear icon for the "EH Pod Network (static)" profile.

5) Then on the IPv4 tab update the Address and Gateway so the third octet matches your pod number.

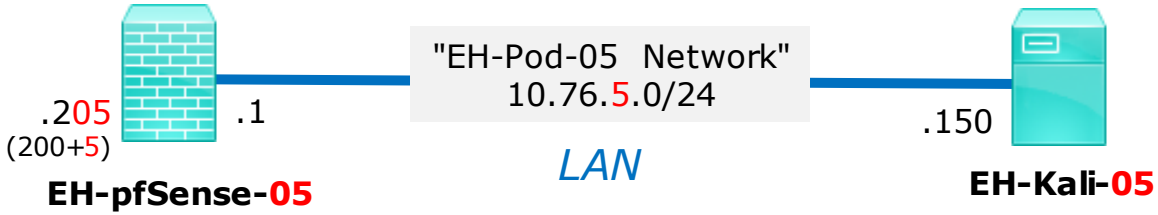
Example: Configuring the EH-Kali VM in EH-Pod-05

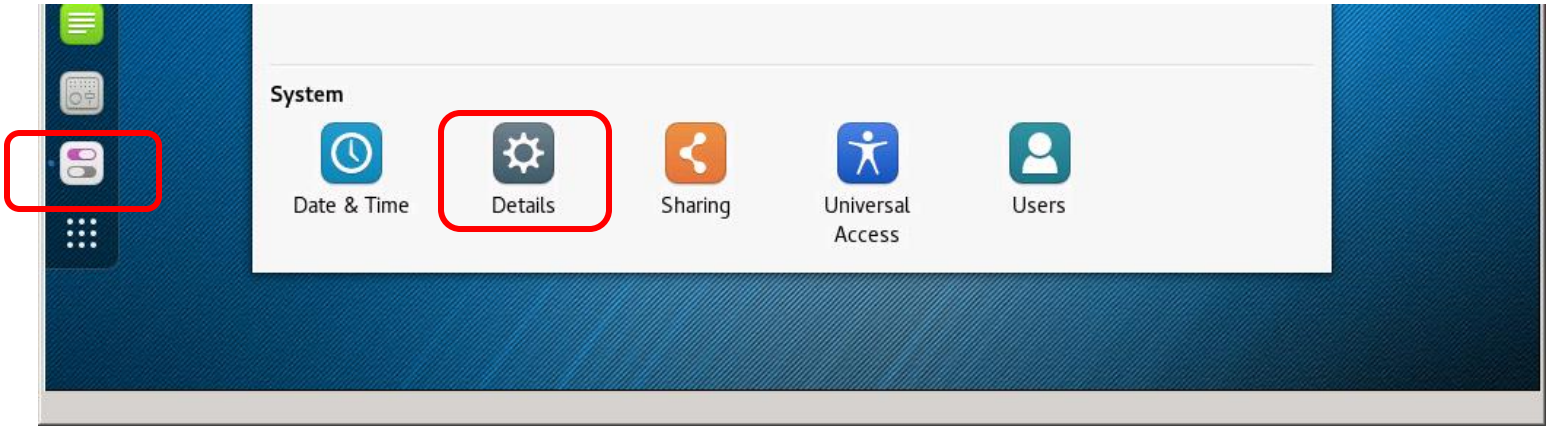




6) Click on the EH Pod Network (static) profile and make sure you see the updated IPv4 address and Default Route. Then close the Network dialog box.

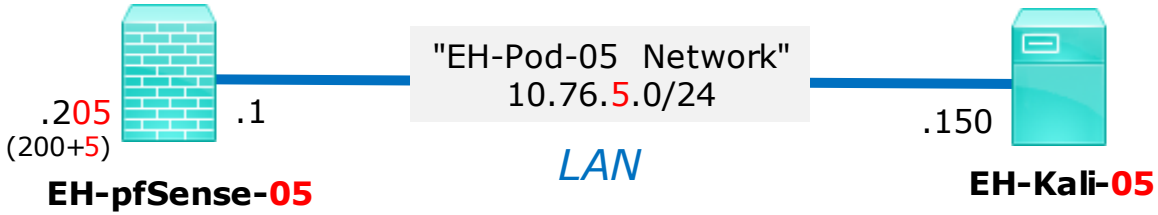
Example: Configuring the EH-Kali VM in EH-Pod-05





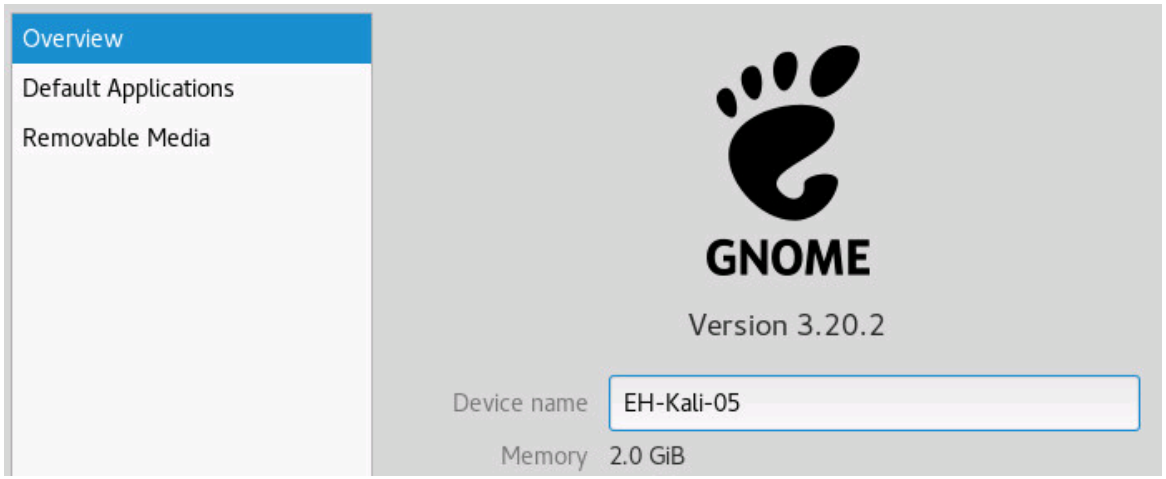
7) Click the Settings icon on the left panel then the Details icon on the All Settings dialog box.

Example: Configuring the EH-Kali VM in EH-Pod-05



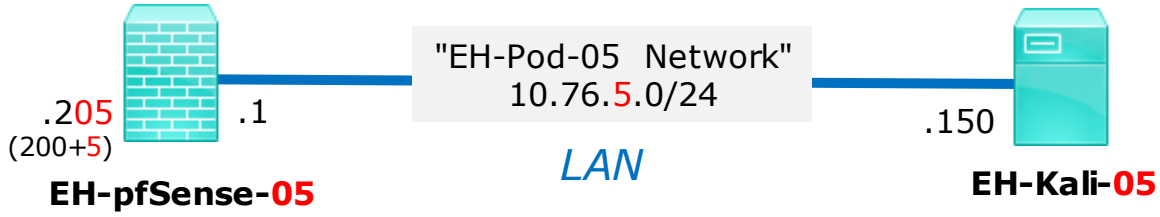
This example shows pod 5.

Each student should only use the pod assigned to them.



8) Update the device name to EH-Kali-xx, where xx is your 2 digit pod number.

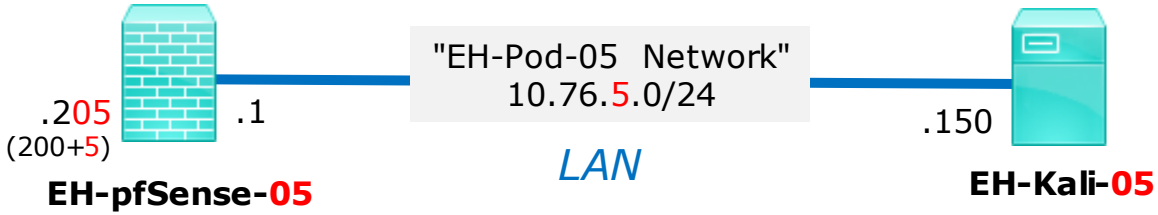
Example: Configuring the EH-Kali VM in EH-Pod-05

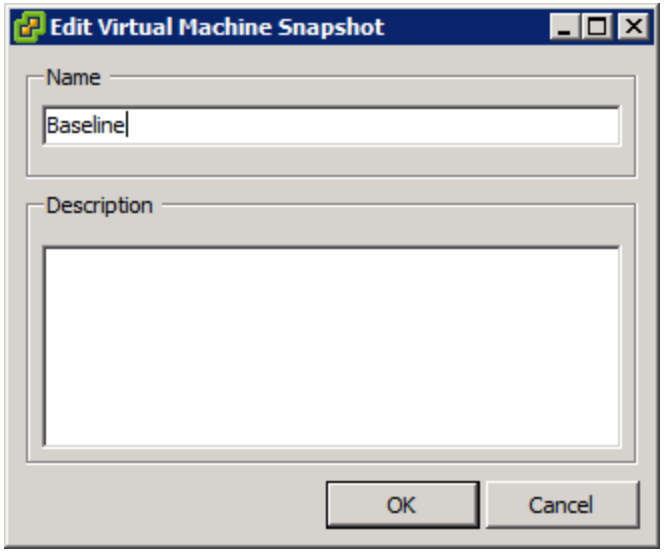



```
root@eh-kali-05: ~
File  Edit  View  Search  Terminal  Help
root@eh-kali-05:~# ping opus.cis.cabrillo.edu -c2
PING oslab.cis.cabrillo.edu (172.30.5.20) 56(84) bytes of data.
64 bytes from opus.cis.cabrillo.edu (172.30.5.20): icmp_seq=1 ttl=62 time=0.879 ms
64 bytes from opus.cis.cabrillo.edu (172.30.5.20): icmp_seq=2 ttl=62 time=1.24 ms

--- oslab.cis.cabrillo.edu ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.879/1.060/1.242/0.184 ms
root@eh-kali-05:~# ping google.com -c2
PING google.com (216.58.194.174) 56(84) bytes of data.
64 bytes from sfo07s13-in-f14.1e100.net (216.58.194.174): icmp_seq=1 ttl=56 time=3.95 ms
64 bytes from sfo07s13-in-f14.1e100.net (216.58.194.174): icmp_seq=2 ttl=56 time=4.18 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 3.953/4.070/4.188/0.133 ms
root@eh-kali-05:~#
```

9) Bring up a terminal and verify the prompt shows the correct hostname and you can ping Opus and Google. Note, this requires your pfSense VM to be configured and running.

Example: Configuring the EH-Kali VM in EH-Pod-05



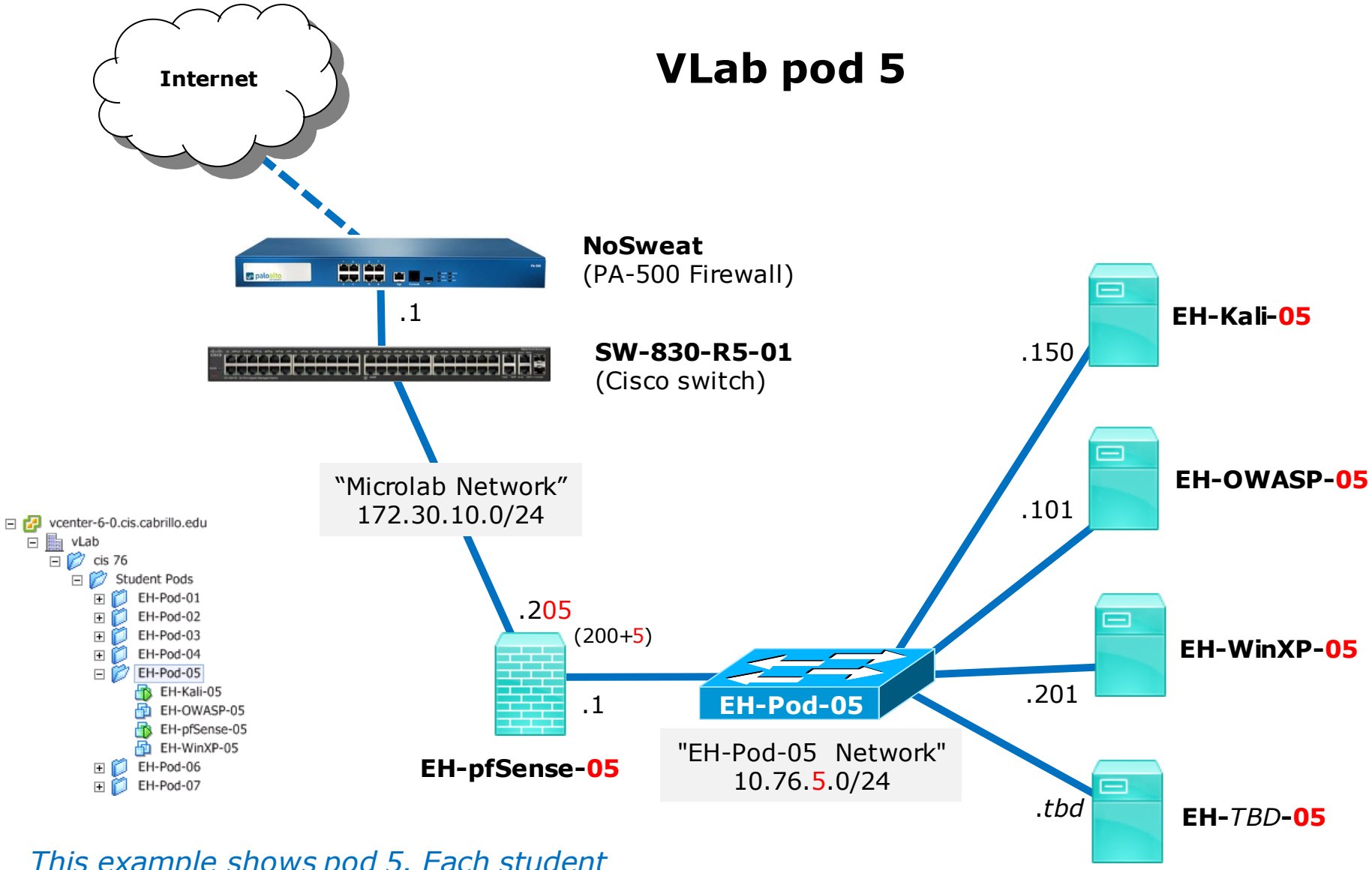


Save your work

Shutdown VM and make a second snapshot named Baseline

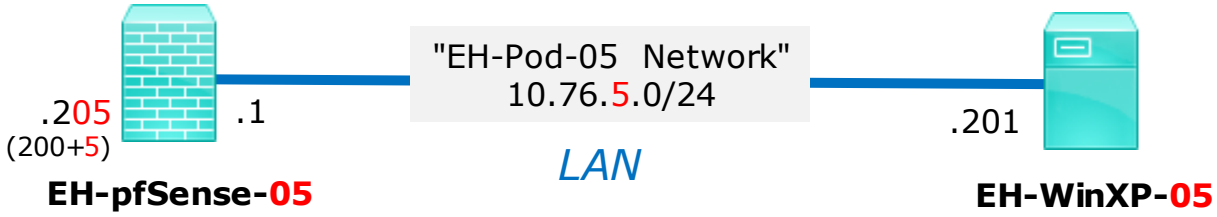
WinXP VM Config

VLab pod 5



This example shows pod 5. Each student should only use the pod assigned to them.

Example: Configuring the EH-WinXP VM in EH-Pod-05

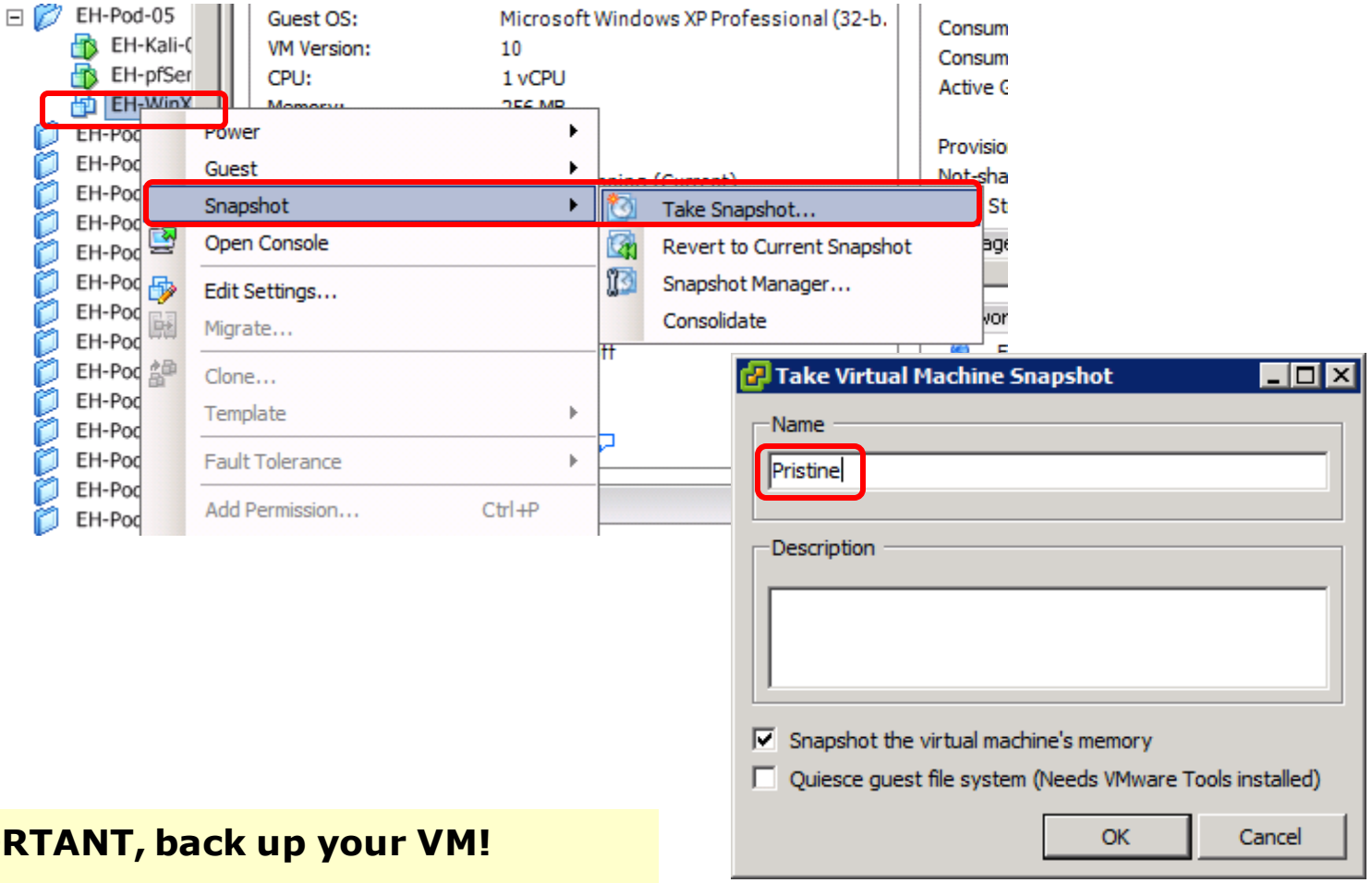


This example shows pod 5.

Each student should only use the pod assigned to them.

WinXP VM	Pod 5 settings
VM Network Adapter 1	EH-Pod-05 Net
Computer Name	EH-WinXP-05
IPv4 address	10.76.5.201
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.5.1

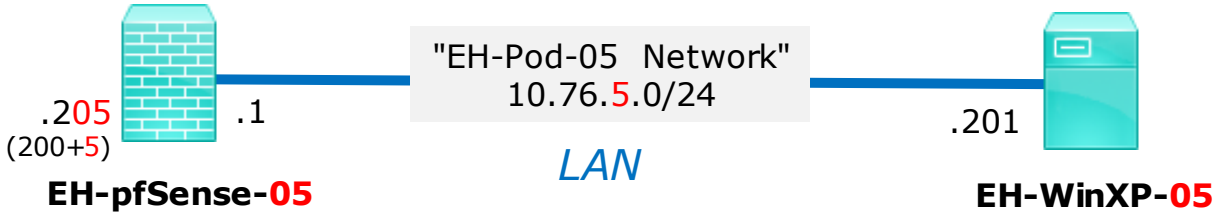
Example: Configuring the EH-WinXP VM in EH-Pod-05

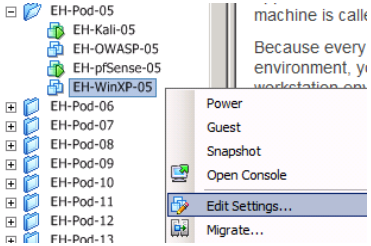


IMPORTANT, back up your VM!

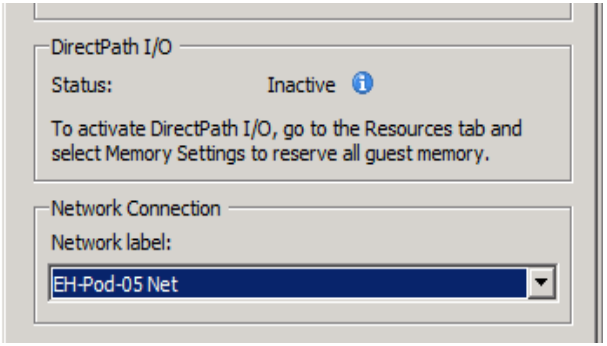
1) Make a backup snapshot of your WinXP VM named "Pristine".

Example: Configuring the EH-WinXP VM in EH-Pod-05





This example shows pod 5. Each student should only use the pod assigned to them.

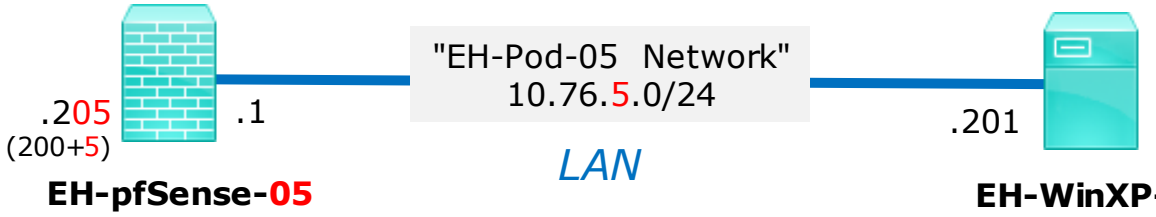


Network Cabling

1) Edit the settings of your WinXP VM.

2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

Example: Configuring the EH-WinXP VM in EH-Pod-05

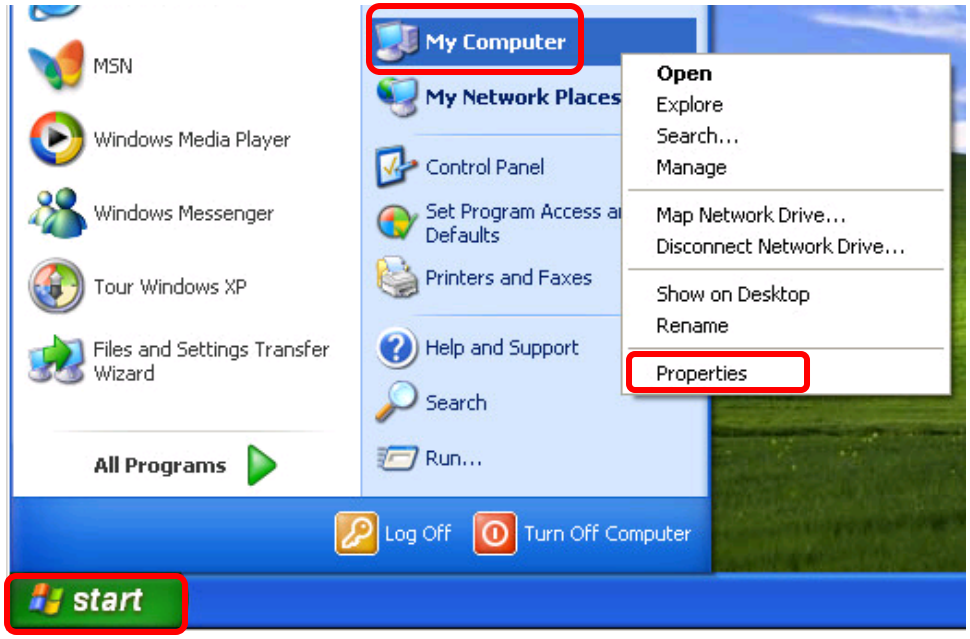


Computer Name Configuration

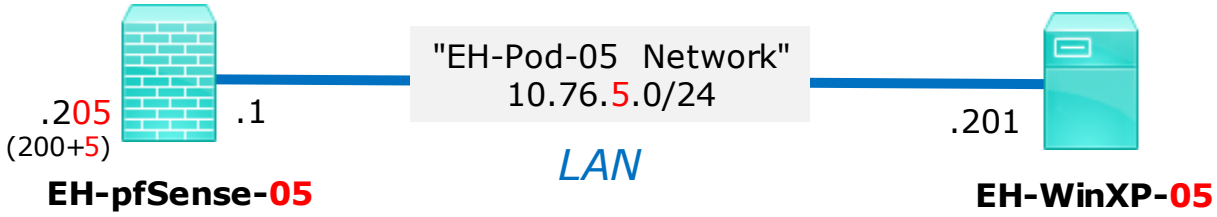
1) Power up the VM and open a console.

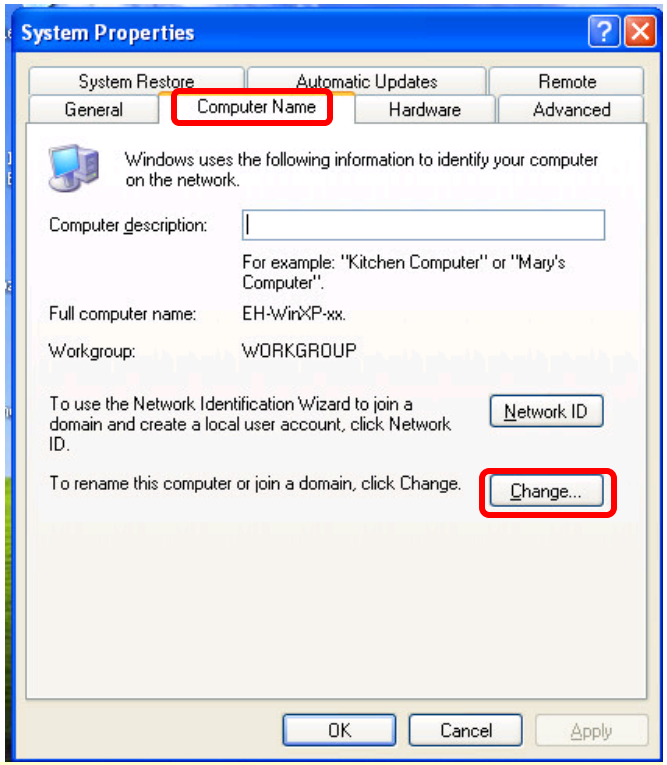
2) Login as the cis76 student user.

3) Click Start, right-click on My Computer and Select Properties.

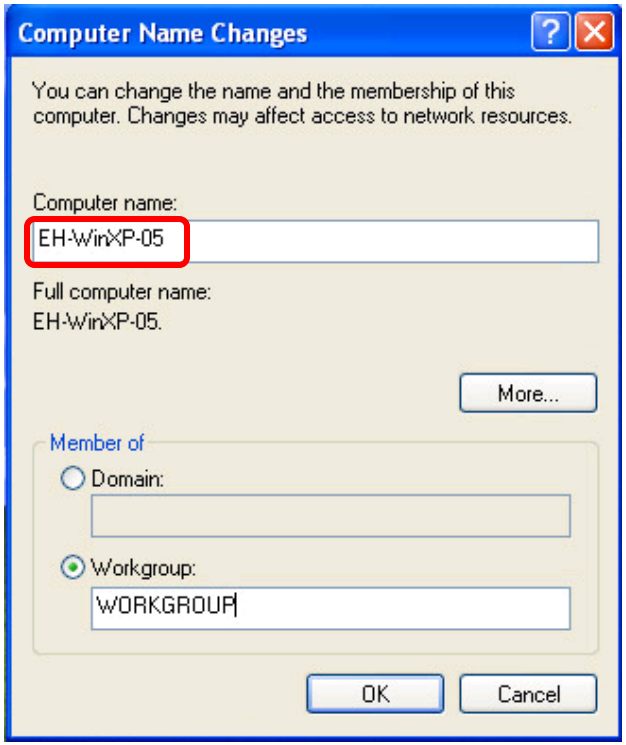


Example: Configuring the EH-WinXP VM in EH-Pod-05



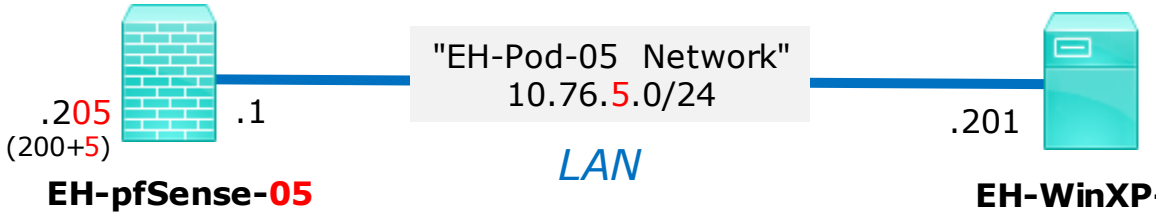


4) Click the Computer Name tab then click Change.



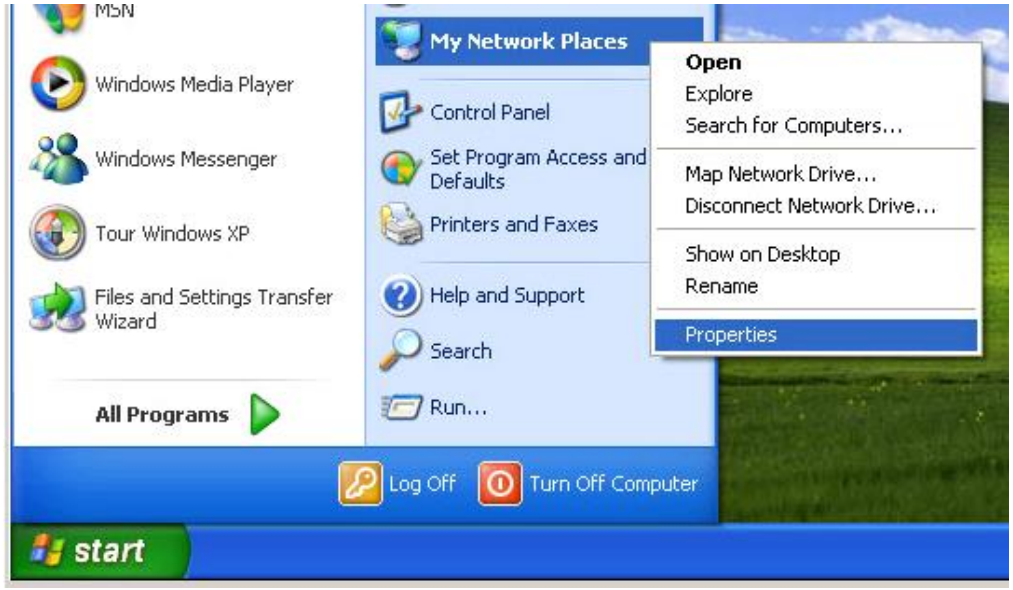
5) Update the Computer name with your two digit pod number. Click Ok and restart the VM.

Example: Configuring the EH-WinXP VM in EH-Pod-05

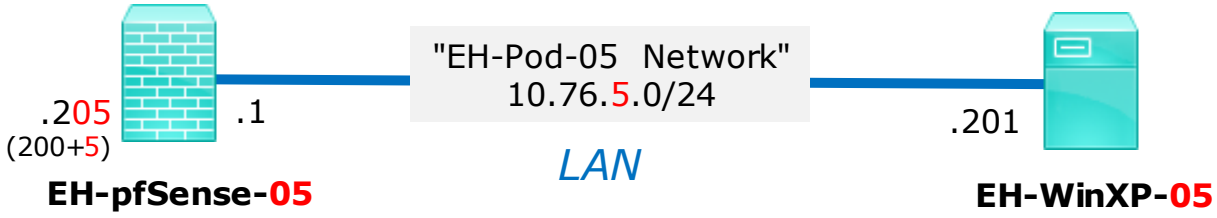


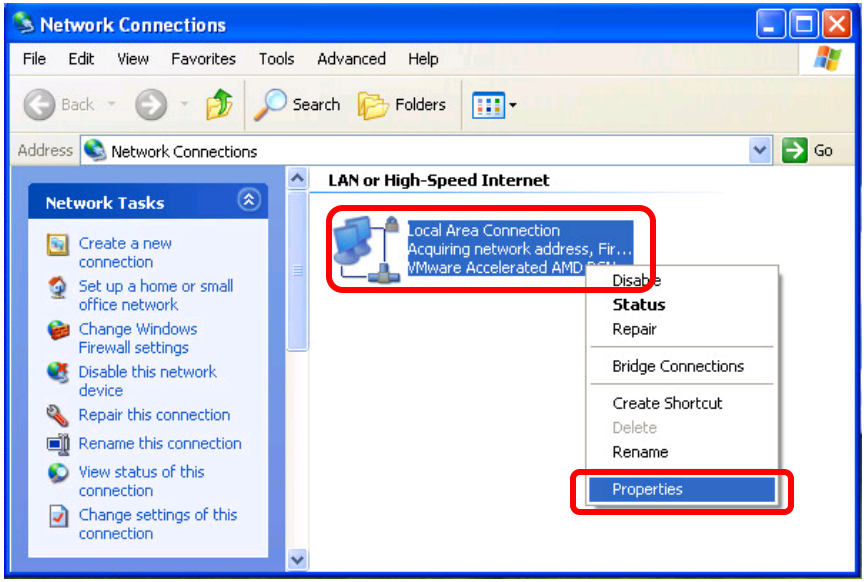
Network Configuration

1) Click Start, right-click on My Network Places and Select Properties.

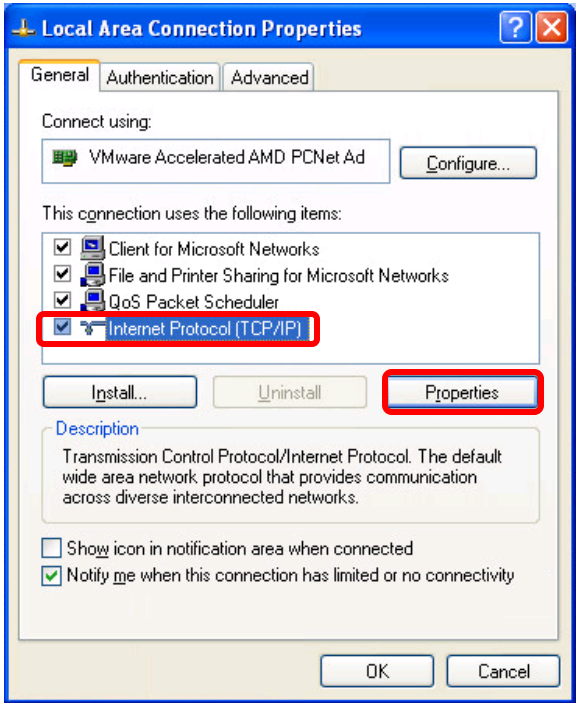


Example: Configuring the EH-WinXP VM in EH-Pod-05



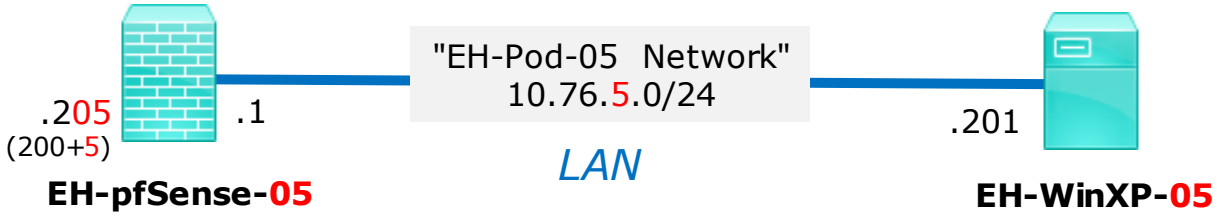


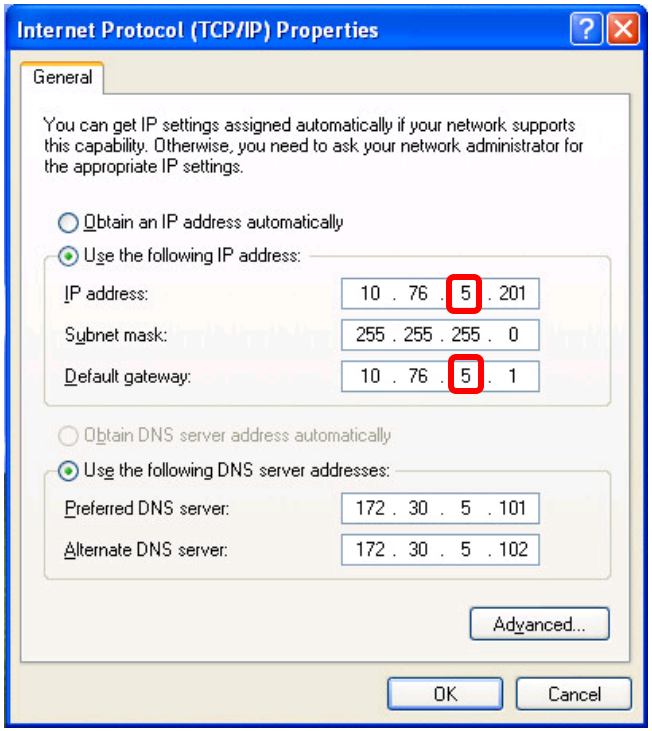
2) Right-click on the Lan Area Connection and Select Properties.



3) Select Internet Protocol (TCP/IP) and click on Properties.

Example: Configuring the EH-WinXP VM in EH-Pod-05

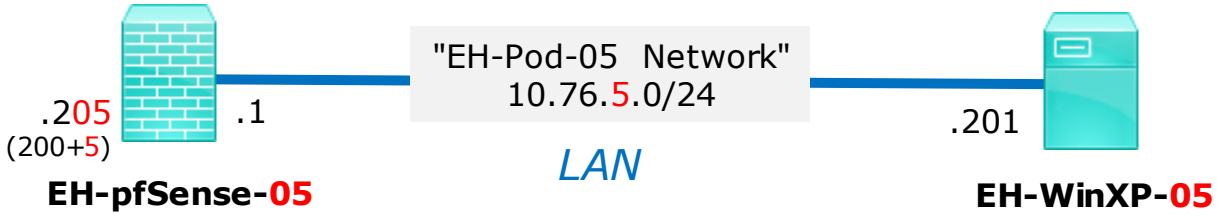


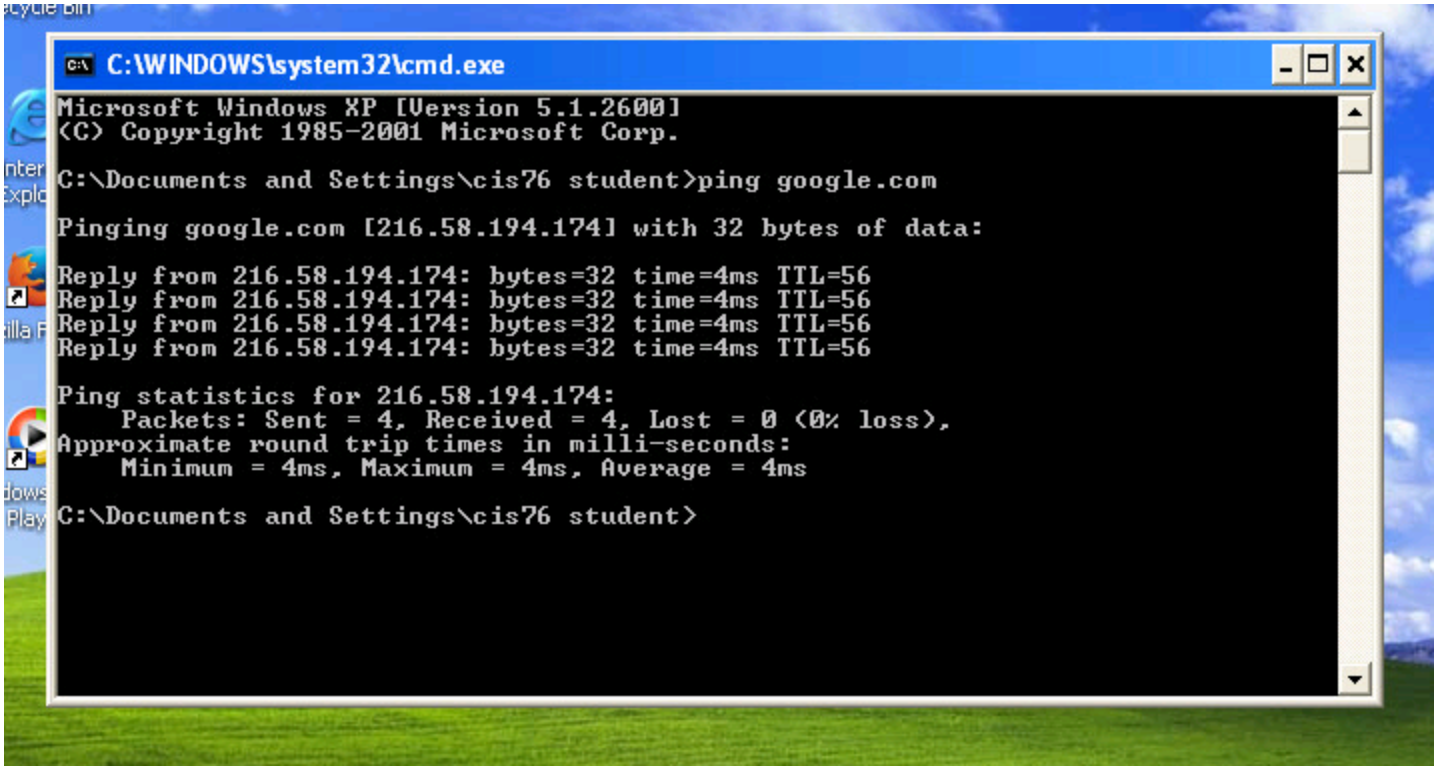


4) Update the third octet of the IP Address and Default Gateway to match your pod number.

5) Click OK and close any open dialog boxes.

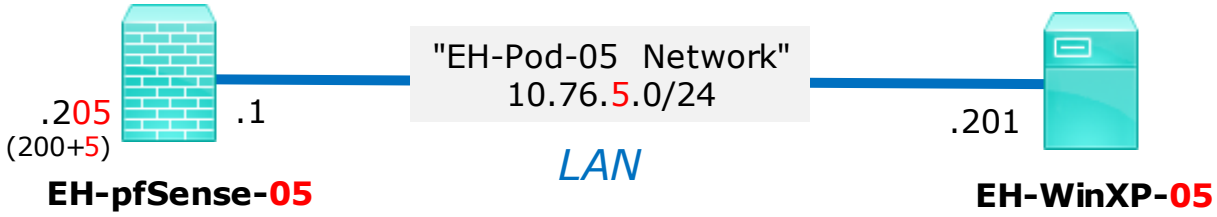
Example: Configuring the EH-WinXP VM in EH-Pod-05

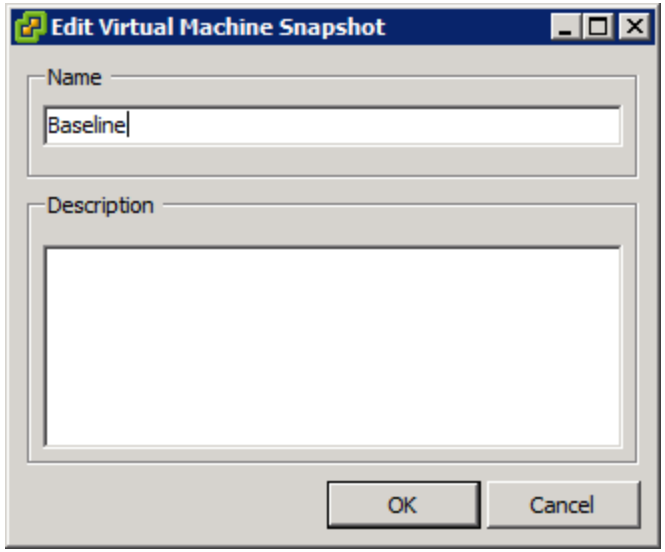




6) Run cmd.exe to bring up a command prompt and ping google.com to verify your network settings.

Example: Configuring the EH-WinXP VM in EH-Pod-05





Save your work

Shutdown VM and make a second snapshot named Baseline

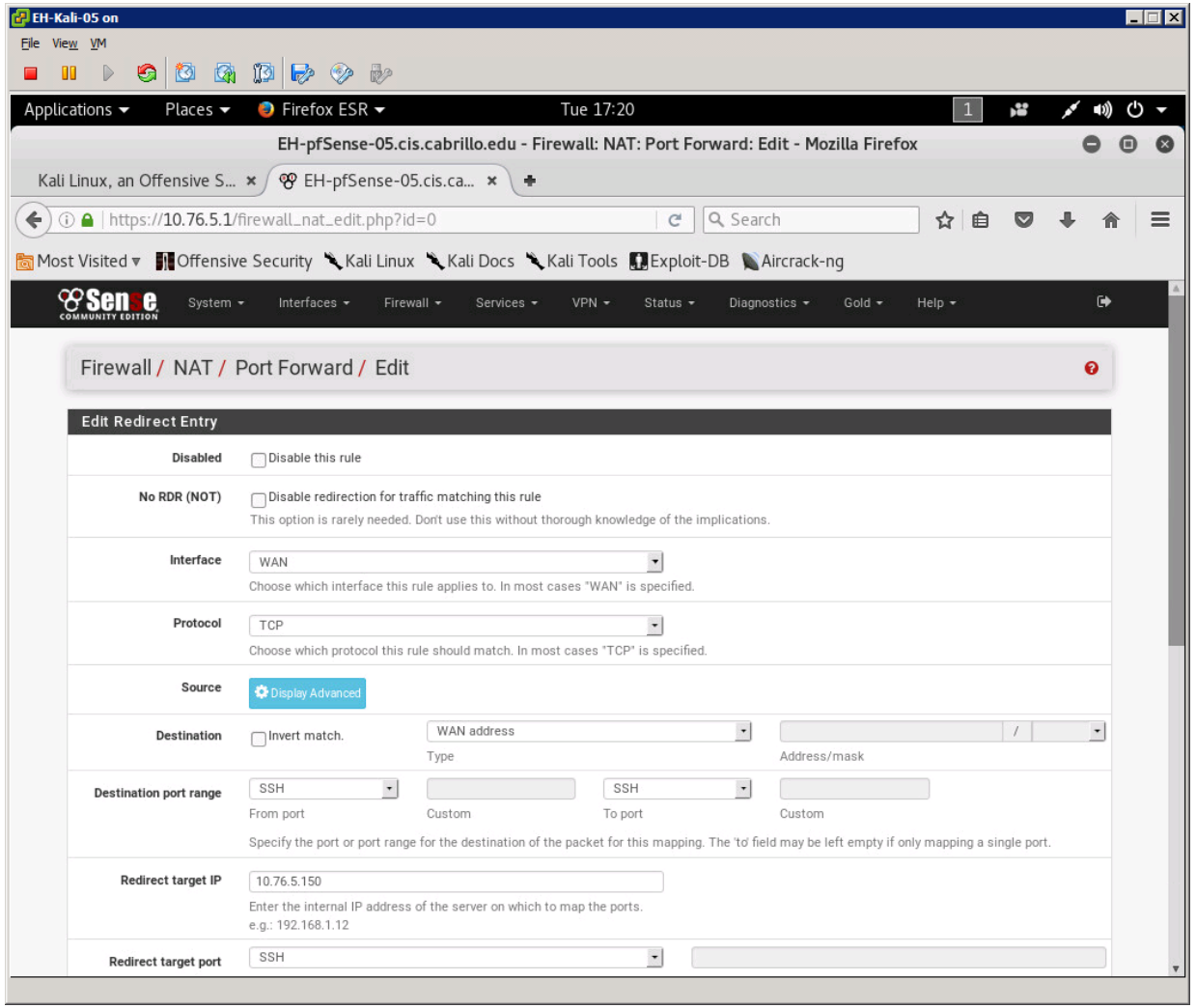
Port Forwarding (optional)

Configure pfSense to forward port 22 to Kali VM

Forward SSH through pfSense Firewall to Kali VM

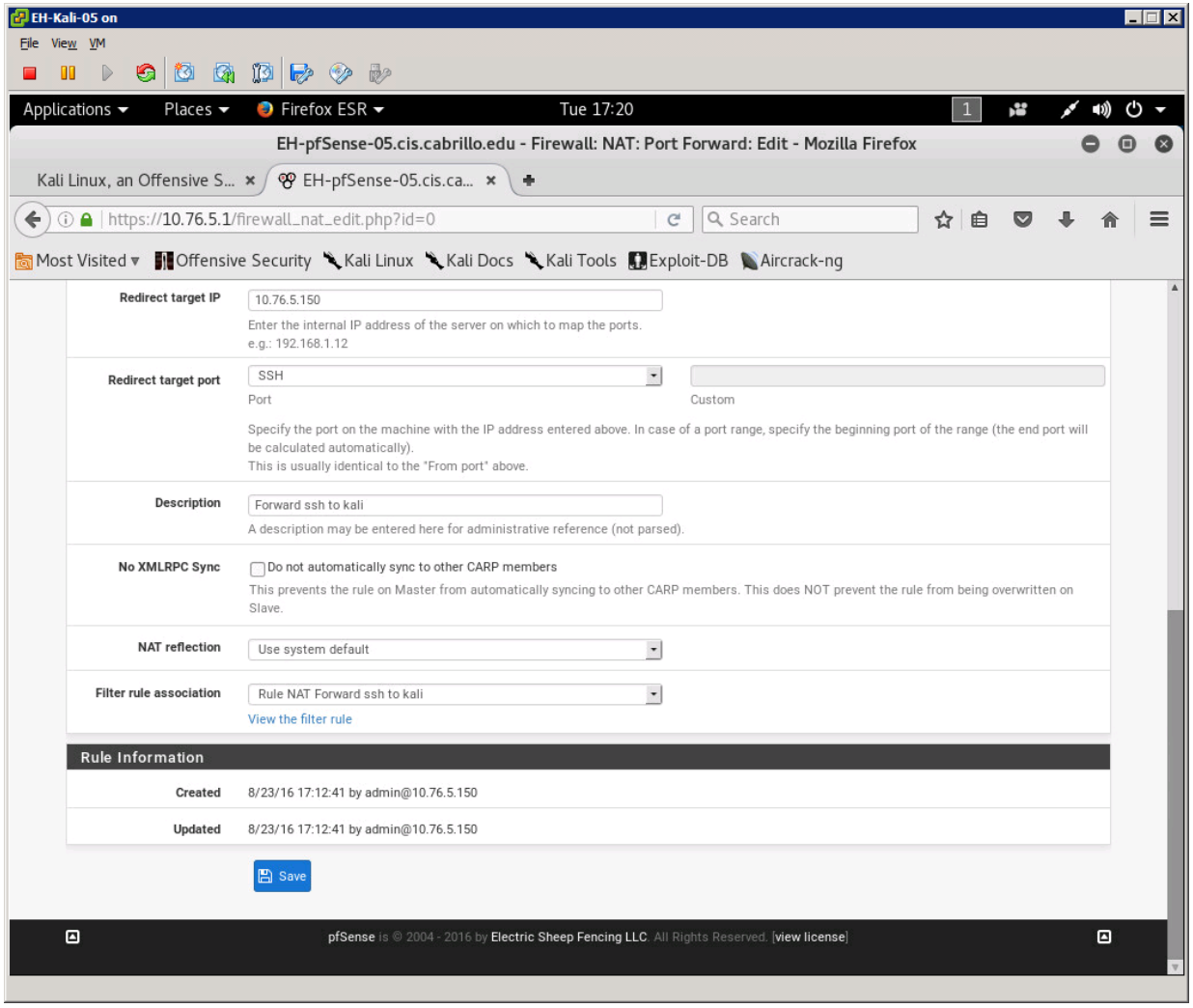
See: https://doc.pfsense.org/index.php/How_can_I_forward_ports_with_pfSense

Forward SSH through pfSense Firewall to Kali



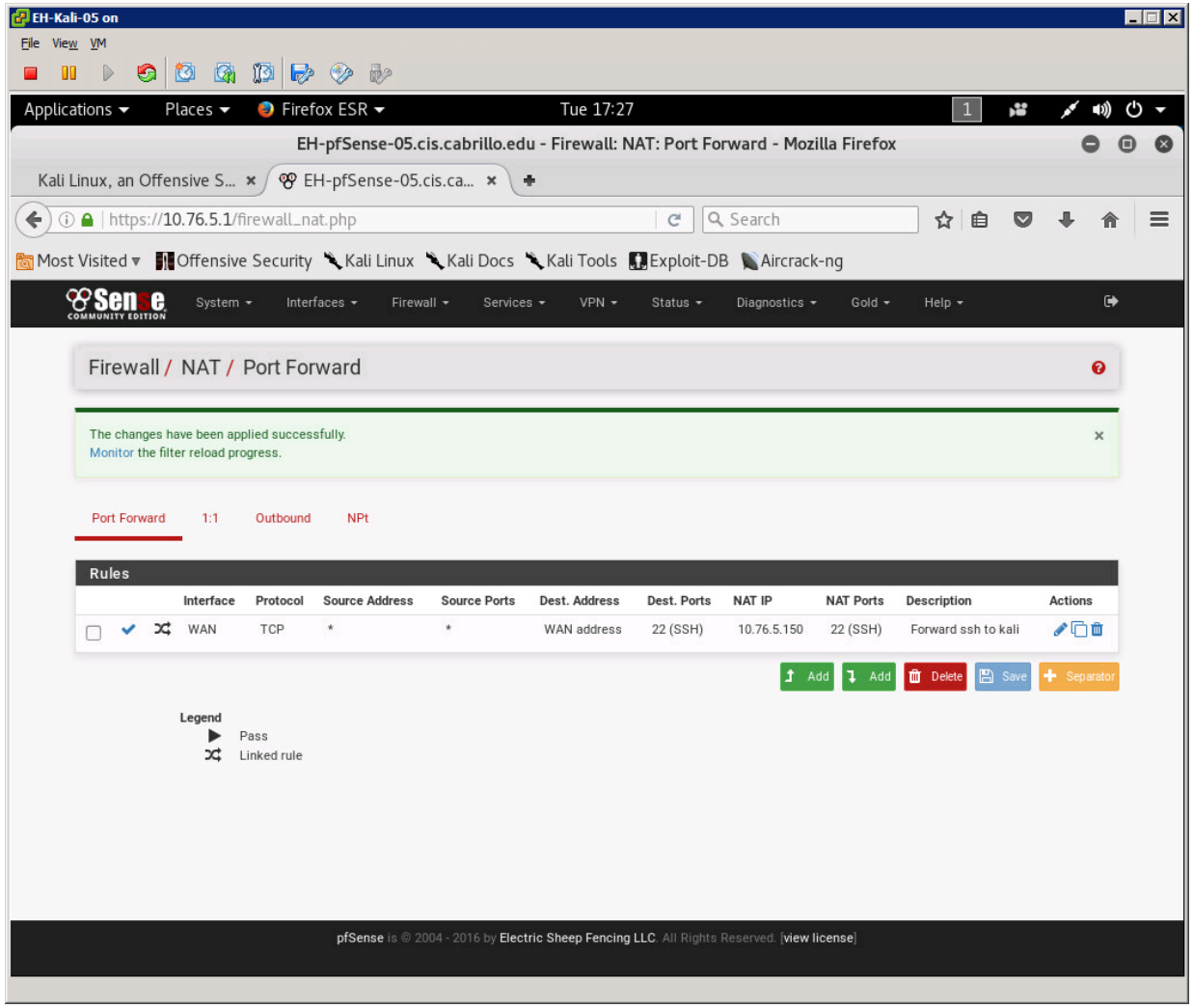
This example is for Pod 5

Forward SSH through pfSense Firewall to Kali



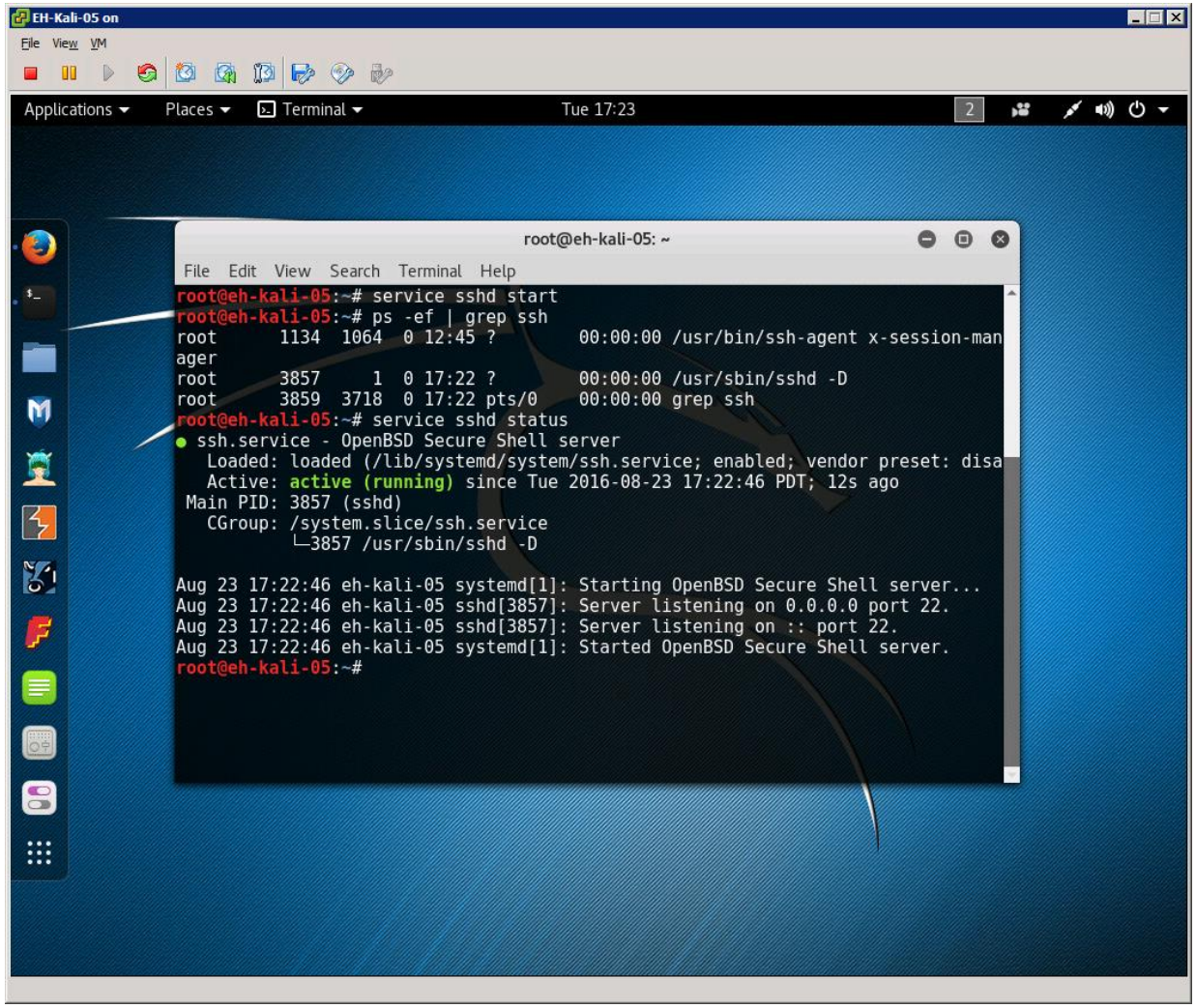
Zoom in to see settings

Forward SSH through pfSense Firewall to Kali

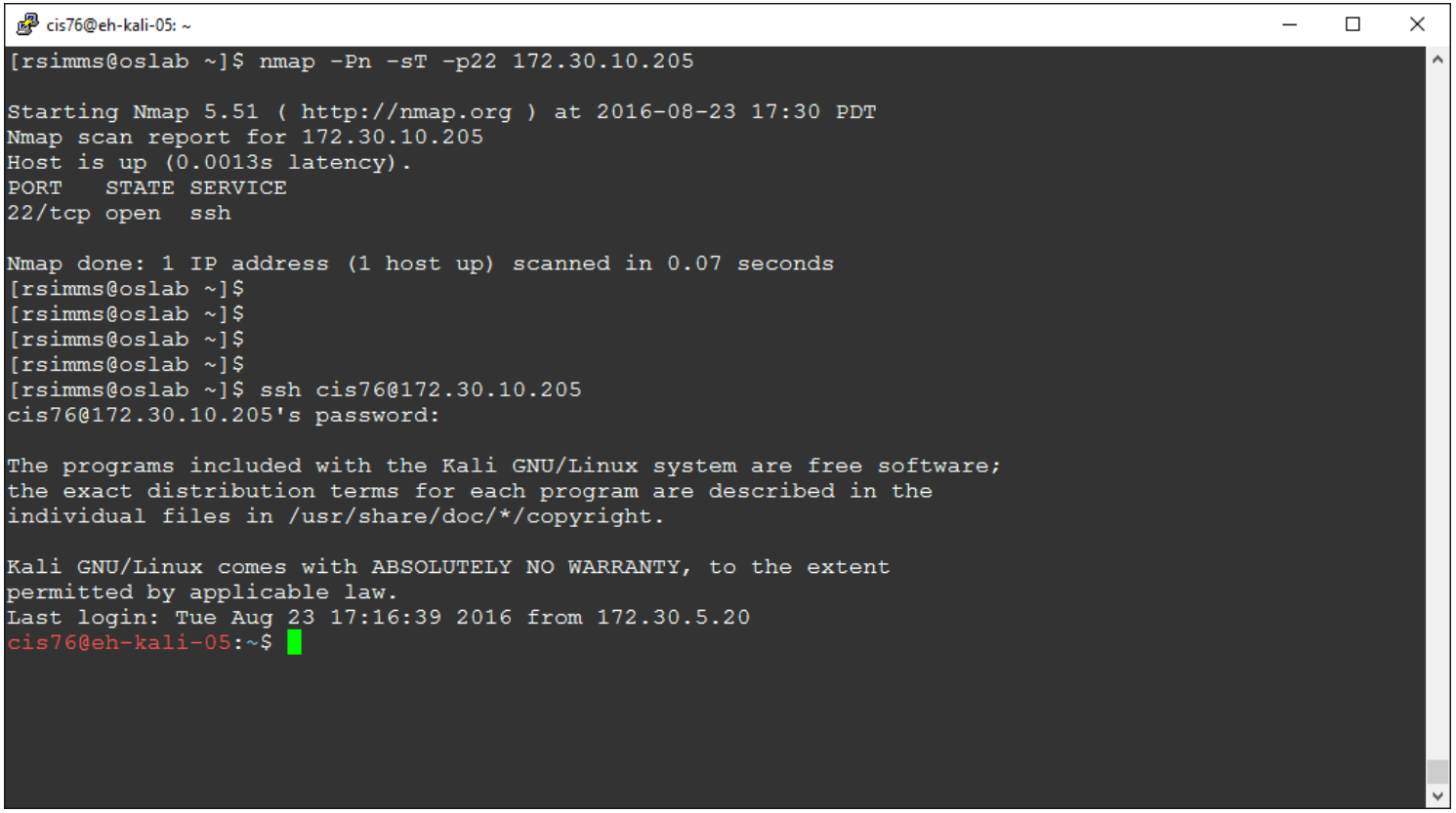


Don't forget to save your changes and apply them

Forward SSH through pfSense Firewall to Kali



Start the ssh serve on Kali

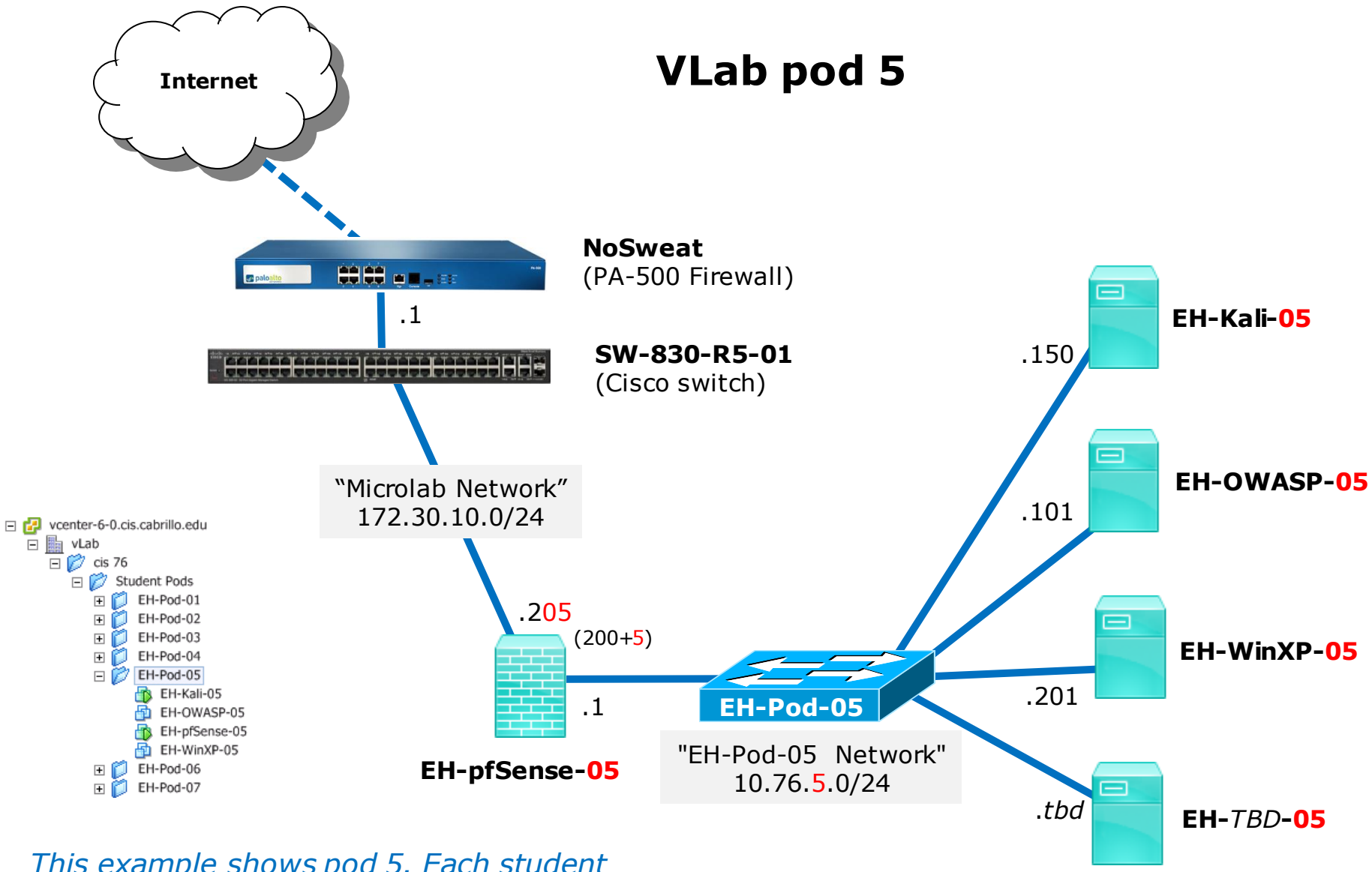


You can now use your favorite terminal emulator and use copy and paste

Work in Progress

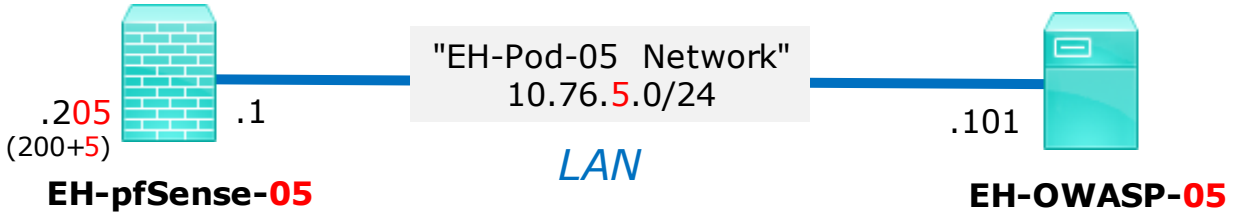
- OWASP VM config

OWASP VM Config



This example shows pod 5. Each student should only use the pod assigned to them.

Example: Configuring the EH-OWASP VM in EH-Pod-05

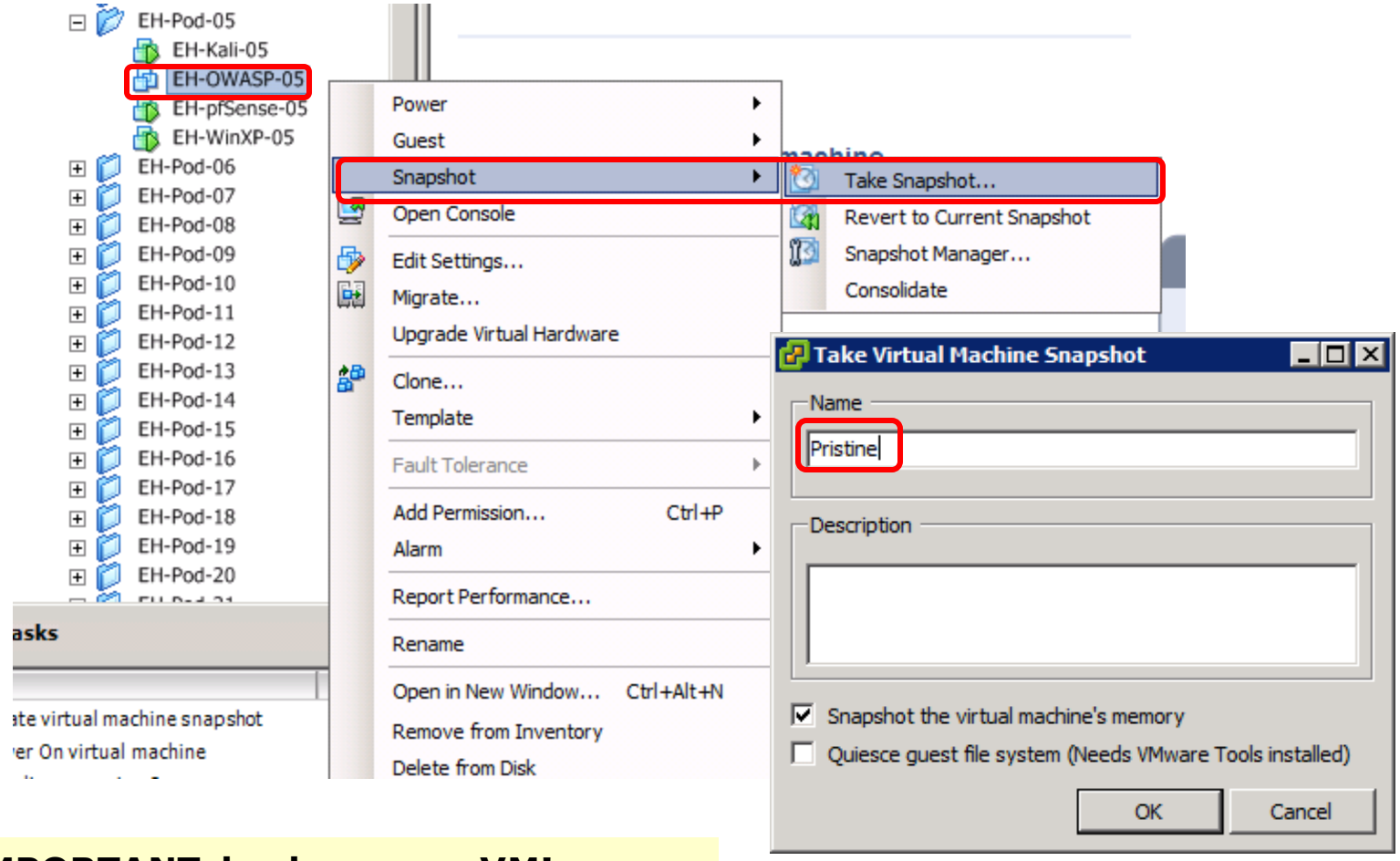


This example shows pod 5.

Each student should only use the pod assigned to them.

OWASP VM	Pod 5 settings
VM Network Adapter 1	EH-Pod-05 Net
IPv4 address	10.76.5.101
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.5.1
DNS domain search	cis.cabrillo.edu
DNS name servers	172.30.5.101 172.30.5.102

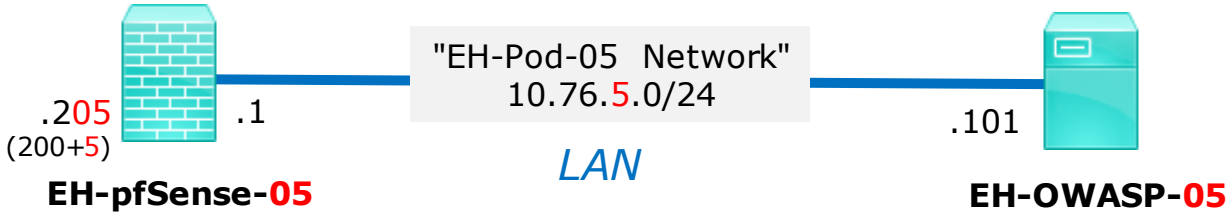
Example: Configuring the EH-OWASP VM in EH-Pod-05

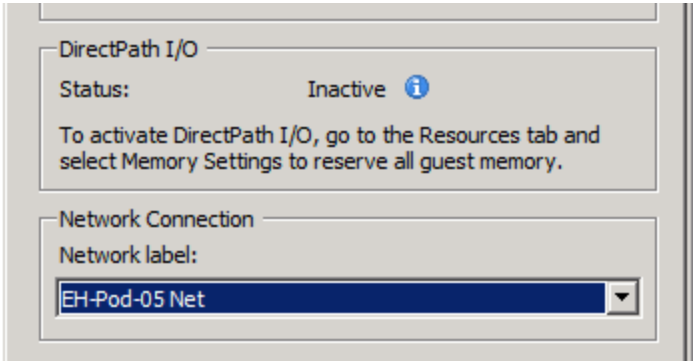


IMPORTANT, back up your VM!

1) Make a backup snapshot of your OWASP VM named "Pristine".

Example: Configuring the EH-OWASP VM in EH-Pod-05



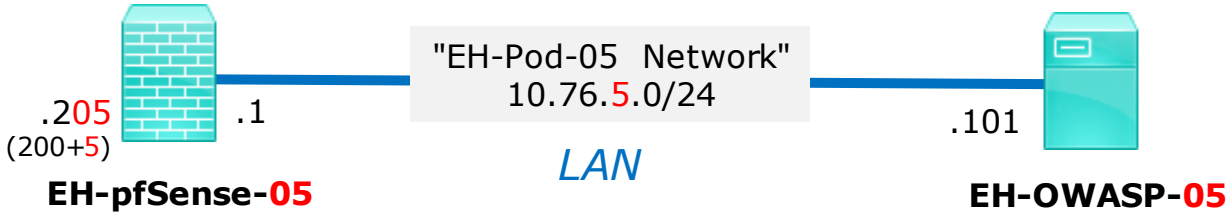


Network Cabling

1) Edit the settings of your OWASP VM.

2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

Example: Configuring the EH-OWASP VM in EH-Pod-05



Network Configuration

1) Power up the VM and open a console.

2) Login as the root user.

3) Edit /etc/network/interfaces:

a) Modify the third octet of the IP address and gateway to your pod number.

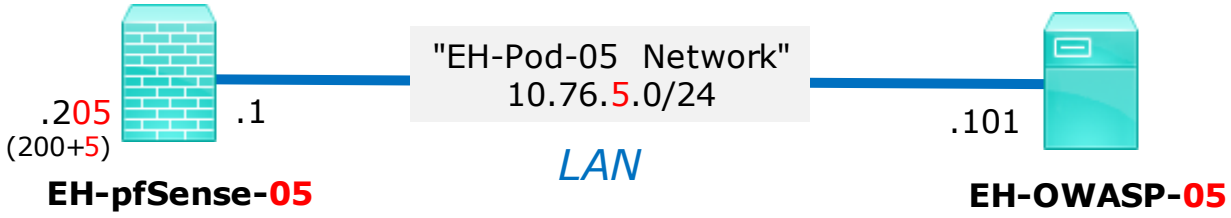
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
  address 10.76.5.101
  netmask 255.255.255.0
  gateway 10.76.5.1

dns-search cis.cabrillo.edu
dns-nameservers 172.30.5.101 172.30.5.102
```

b) Add: **dns-search cis.cabrillo.edu**

c) Add: **dns-nameservers 172.30.5.101 172.30.5.102**

d) Save and exit.

Example: Configuring the EH-OWASP VM in EH-Pod-05



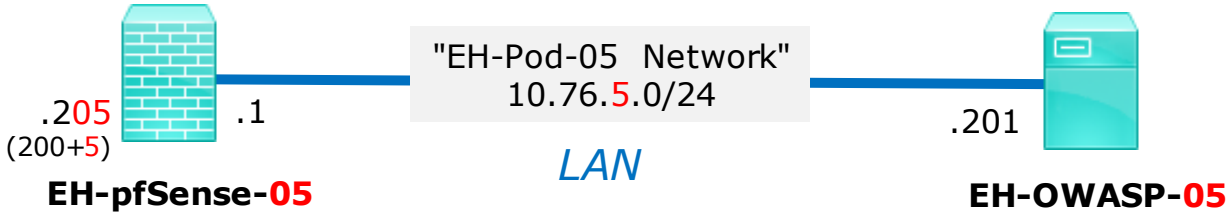
4) Restart networking with:
/etc/init.d/networking restart

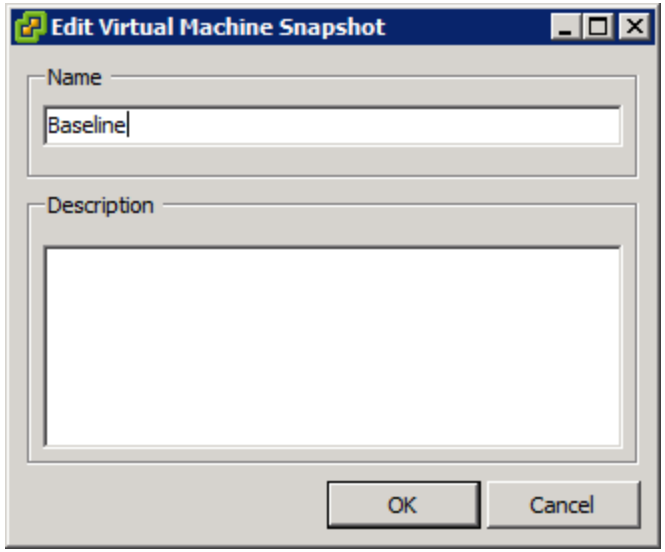
5) Verify the third octet of your IP address matches your pod number.

6) Verify Internet access.

```
root@owaspbwa:~# /etc/init.d/networking restart
 * Reconfiguring network interfaces...
ssh stop/waiting
ssh start/running, process 2231
                                                                [ OK ]
root@owaspbwa:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:af:63:bb
          inet addr:10.76.5.101  Bcast:10.76.5.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feaf:63bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6447 (6.4 KB)  TX bytes:6410 (6.4 KB)
          Interrupt:18 Base address:0x1400

root@owaspbwa:~# ping google.com -c2
PING google.com (216.58.194.206) 56(84) bytes of data.
64 bytes from sfo03s01-in-f14.1e100.net (216.58.194.206): icmp_seq=1 ttl=55 time
=4.77 ms
64 bytes from sfo03s01-in-f206.1e100.net (216.58.194.206): icmp_seq=2 ttl=55 tim
e=4.96 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 4.776/4.872/4.968/0.096 ms
root@owaspbwa:~#
```

Example: Configuring the EH-OWASP VM in EH-Pod-05





Save your work

Shutdown VM and make a second snapshot named Baseline