

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

<http://simms-teach.com/>

Rich's Cabrillo College CIS Classes
Home Page

Home Resources Forums CIS Lab Canvas

Login
Flashcards
Admin

CIS 76
CIS 90
Previous Terms

10 days till term starts!

Cabrillo College
Web Advisor
Blackboard
Commands and Files

VLab (classic)
VLab (web)
NETLAB+

CIS 76 VLab Pod Assignments

CIS 90 VLab VM Assignments

RIP Dennis Ritchie

Opus Status: UP

Metal Sitemap W3C XHTML 1.0 W3C CSS Credits Earth

CIS 76 VLab Assignments	
Abraham	Pod 21
Abraham	Pod 22
Abraham	Pod 23
Abraham	Pod 24
Abraham	Pod 25
Abraham	Pod 26
Abraham	Pod 27
Abraham	Pod 28
Abraham	Pod 29
Abraham	Pod 30
Abraham	Pod 31
Abraham	Pod 32
Abraham	Pod 33
Abraham	Pod 34
Abraham	Pod 35
Abraham	Pod 36
Abraham	Pod 37
Abraham	Pod 38
Abraham	Pod 39
Abraham	Pod 40
Abraham	Pod 41
Abraham	Pod 42
Abraham	Pod 43
Abraham	Pod 44
Abraham	Pod 45
Abraham	Pod 46
Abraham	Pod 47
Abraham	Pod 48
Abraham	Pod 49
Abraham	Pod 50
Abraham	Pod 51
Abraham	Pod 52
Abraham	Pod 53
Abraham	Pod 54
Abraham	Pod 55
Abraham	Pod 56
Abraham	Pod 57
Abraham	Pod 58
Abraham	Pod 59
Abraham	Pod 60
Abraham	Pod 61
Abraham	Pod 62
Abraham	Pod 63
Abraham	Pod 64
Abraham	Pod 65
Abraham	Pod 66
Abraham	Pod 67
Abraham	Pod 68
Abraham	Pod 69
Abraham	Pod 70
Abraham	Pod 71
Abraham	Pod 72
Abraham	Pod 73
Abraham	Pod 74
Abraham	Pod 75
Abraham	Pod 76
Abraham	Pod 77
Abraham	Pod 78
Abraham	Pod 79
Abraham	Pod 80
Abraham	Pod 81
Abraham	Pod 82
Abraham	Pod 83
Abraham	Pod 84
Abraham	Pod 85
Abraham	Pod 86
Abraham	Pod 87
Abraham	Pod 88
Abraham	Pod 89
Abraham	Pod 90
Abraham	Pod 91
Abraham	Pod 92
Abraham	Pod 93
Abraham	Pod 94
Abraham	Pod 95
Abraham	Pod 96
Abraham	Pod 97
Abraham	Pod 98
Abraham	Pod 99
Abraham	Pod 100

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

Accessing VLab (vSphere Web Client via HTTPS)

[CIS 76](#)
[CIS 90](#)
[Previous Terms](#)

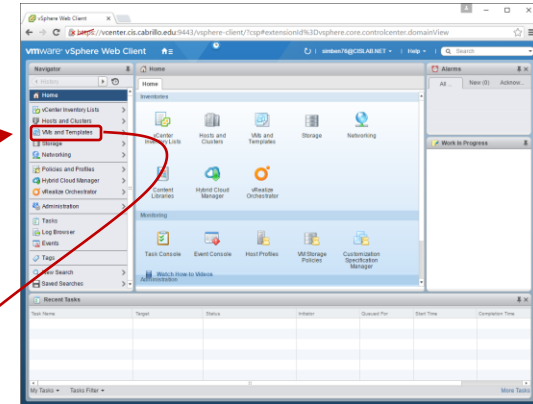
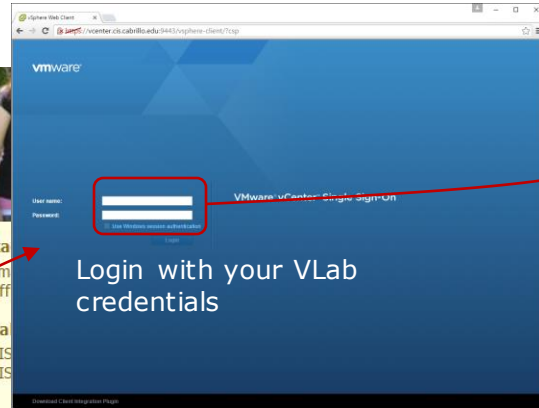
10 days till term starts!

[Cabrillo College](#)
[Web Advisor](#)
[Blackboard](#)
[Commands and Files](#)

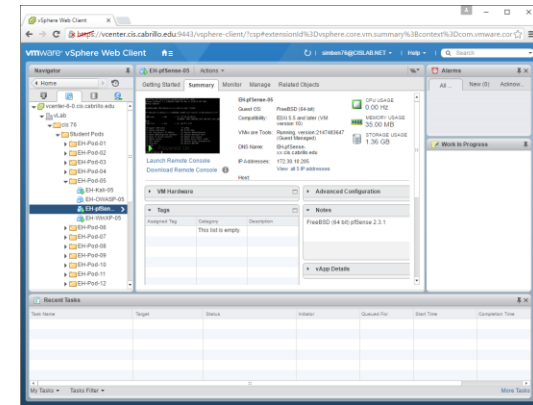
[VLab \(classic\)](#)
[VLab \(web\)](#)
[NETLAB+](#)

[CIS 76 VLab Pod Assignments](#)

[CIS 90 VLab VM Assignments](#)



Select VM and Templates



Expand containers and locate your pod VMs

<http://simms-teach.com/>

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*)

Admin

- CIS 76
- CIS 90
- Previous Terms

10 days till term starts!

Cabrillo College
Web Advisor
Blackboard
Commands and Files

VLab (classic)

VLab (web)
NETLAB+

CIS 76 VLab Pod Assignments

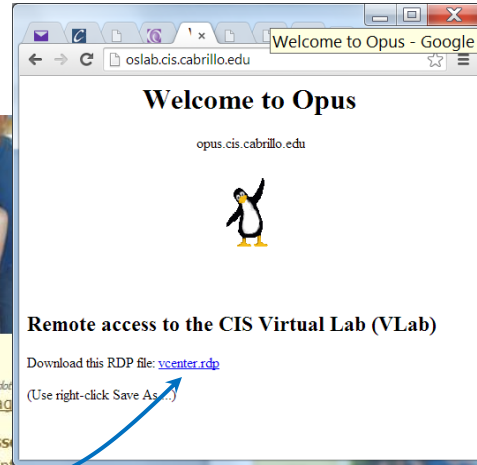
CIS 90 VLab VM Assignments

Contact

- Email: risimms@cabrillo.edu
- Office hours: directory page

My Fall 2016 Cabrillo Classes

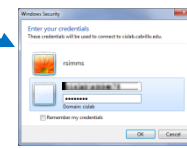
- CIS 76 - Introduction to Information Assurance (lab) - [preview](#)
- CIS 90 Introduction to UNIX/Linux - [preview](#)



1

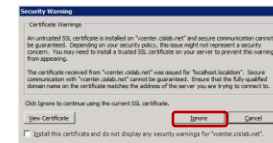


Open



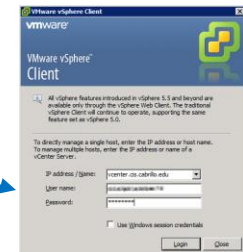
2

Login with VLab credentials

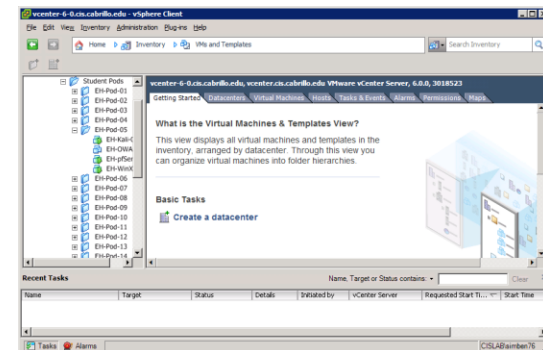


Ignore

Yes, Connect



Wait... **

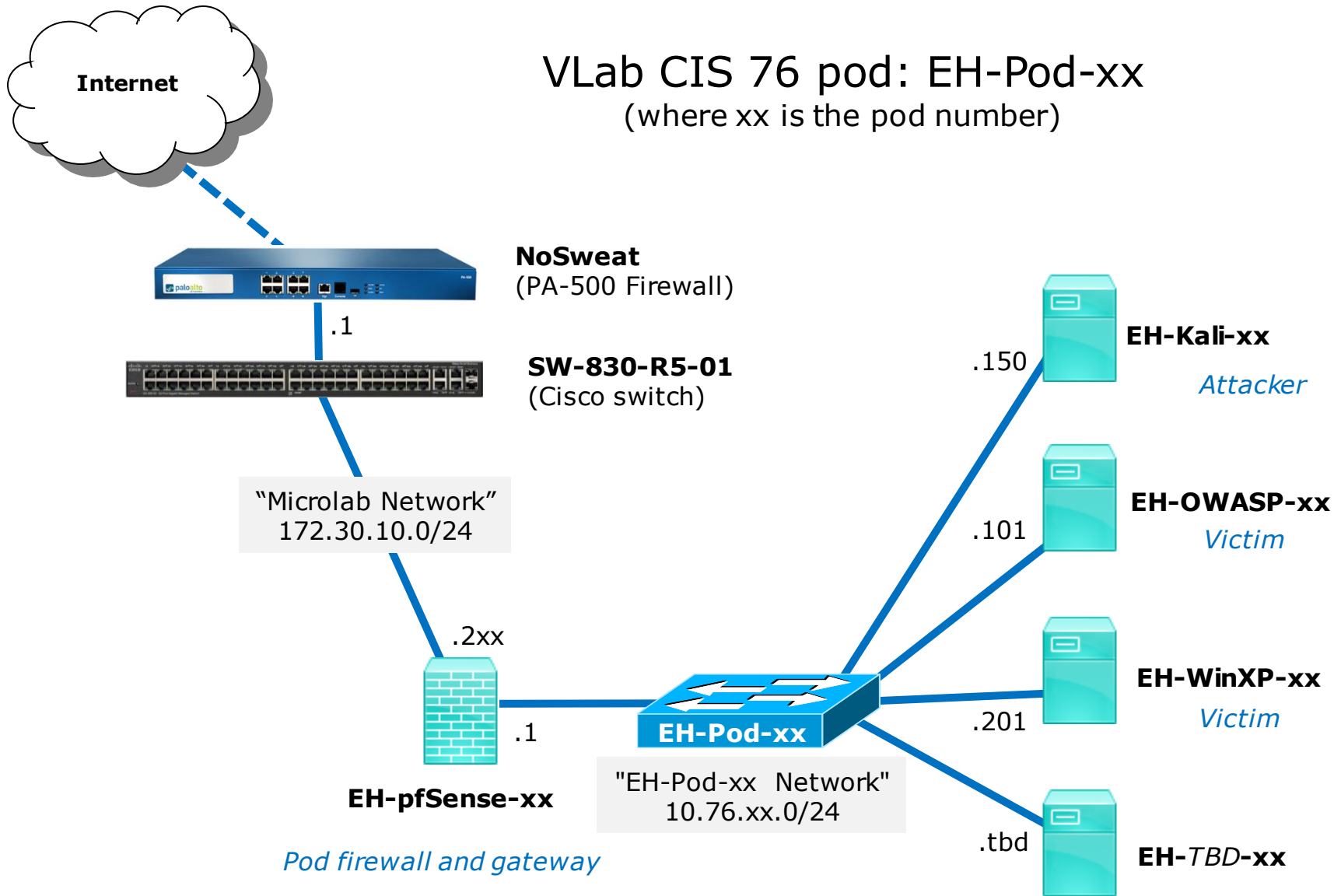


VMs and Templates view

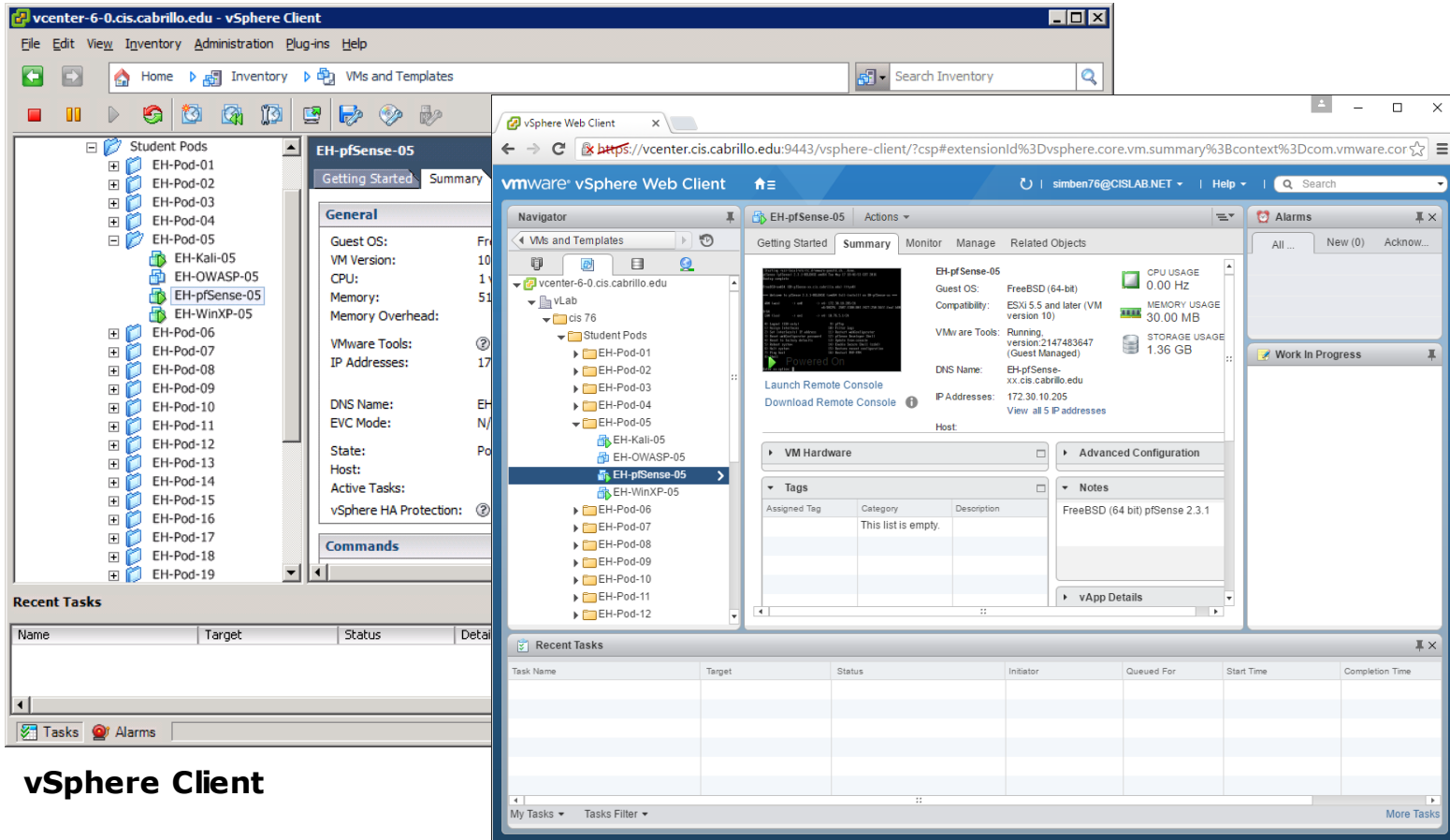
*Mac users will need to install an RDP app like the Microsoft Remote Desktop app.

**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

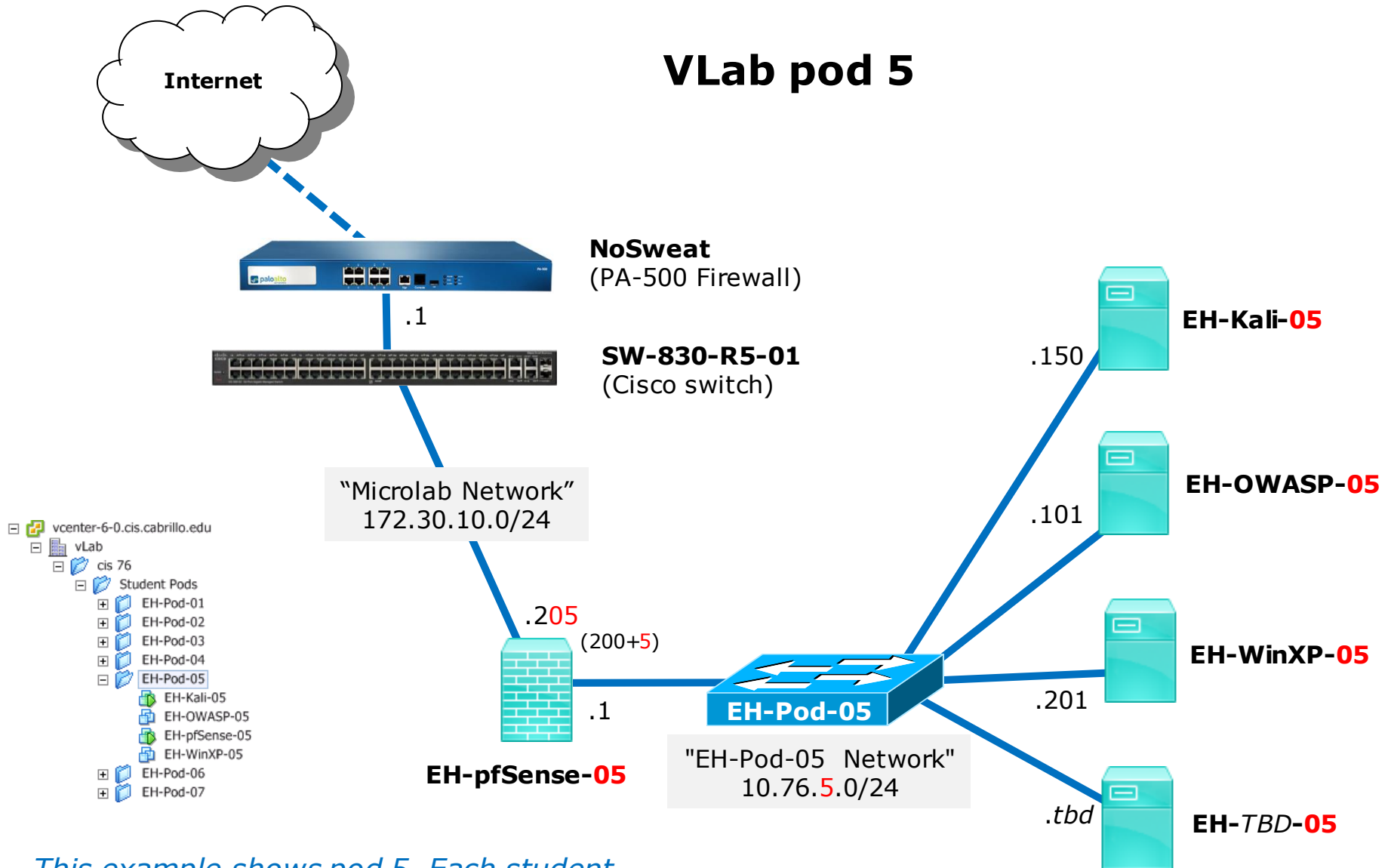
CIS VLab (Virtual Lab) Student Pods

Recent Tasks

Name	Target	Status	Details
Power On virtual machine	EH-pfSense-05	Completed	
Reconfigure virtual machine	EH-pfSense-05	Completed	

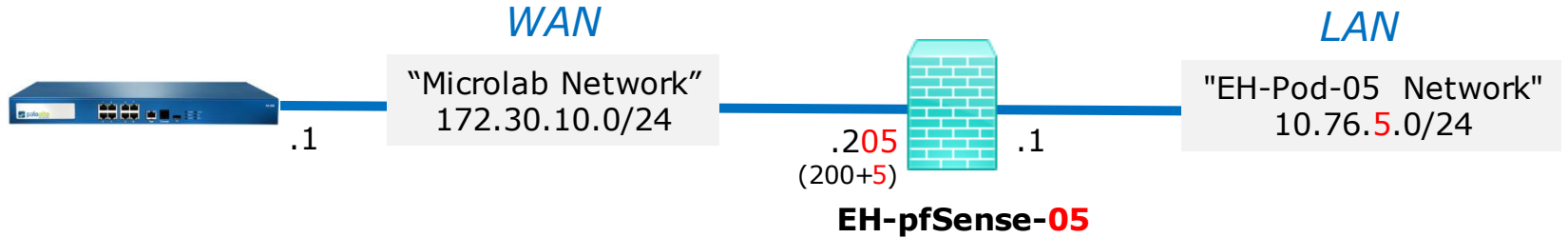
This example shows the pfSense VM in pod 5. Each student should only use the pod assigned to them.

VLab pod 5



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

The screenshot shows the VMware Workstation interface. In the left-hand pane, a tree view lists several virtual machines: EH-Pod-05, EH-Kali-05, EH-pfSense-05, EH-WinXP, EH-Pod-06, EH-Pod-07, EH-Pod-08, EH-Pod-09, EH-Pod-10, EH-Pod-11, and EH-Pod-12. The 'EH-pfSense-05' VM is selected, and its context menu is open. The 'Snapshot' option is highlighted with a red box, and its sub-menu is also open, with 'Take Snapshot...' highlighted by another red box. In the foreground, the 'Take Virtual Machine Snapshot' dialog box is open. The 'Name' field contains the text 'Pristine', which is also highlighted with a red box. The 'Description' field is empty. At the bottom of the dialog, the checkbox 'Snapshot the virtual machine's memory' is checked, and 'Quiesce guest file system (Needs VMware Tools installed)' is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

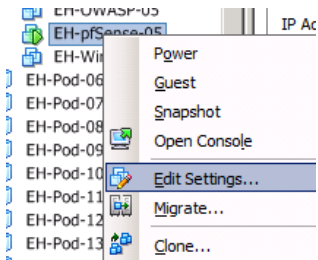
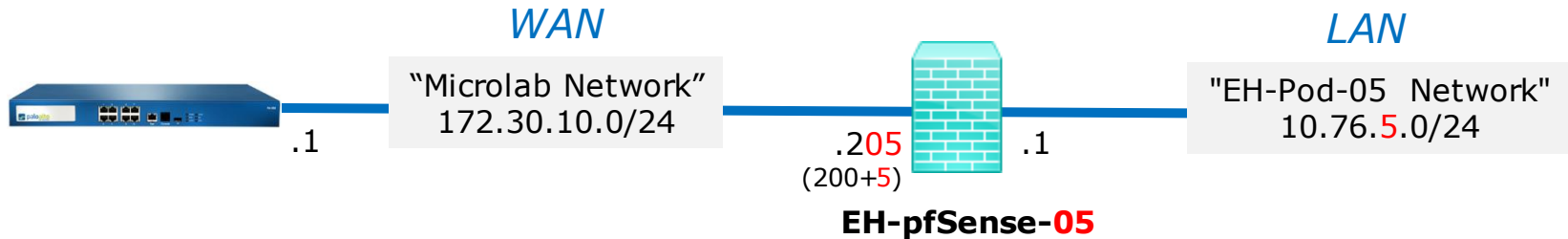
This example shows pod 5.

Each student should only use the pod assigned to them.

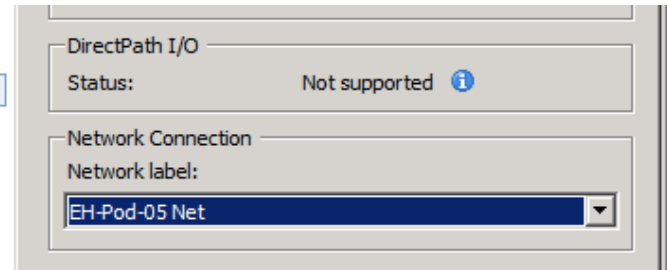
IMPORTANT, back up your VM!

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

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



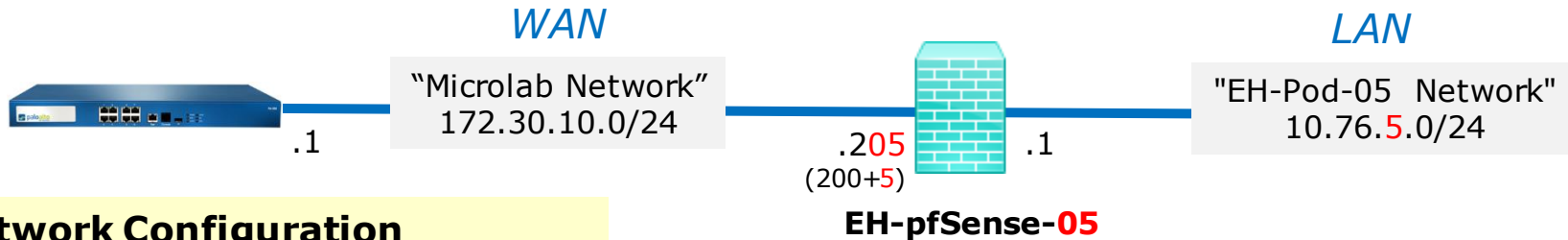
*This example shows pod 5.
Each student should only use
the pod assigned to them.*



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.

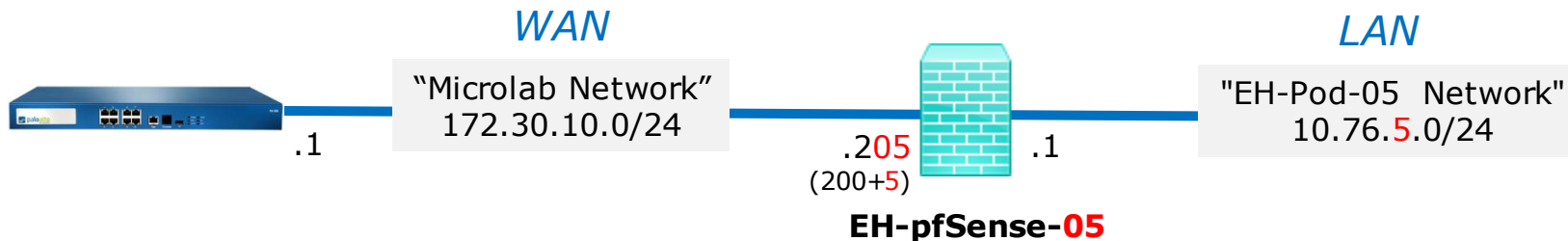
```

EH-pfSense-05 on 172.30.10.20
File View VM
Enter an option:
FreeBSD/amd64 (EH-pfSense-xx.cis.cabrillo.edu) (ttyv0)
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***
WAN (wan)      -> em0      -> v4/DHCP4: 172.30.10.104/24
                v6/DHCP6: 2607:f380:80f:f427:250:56ff:feaf:b80
9/64
LAN (lan)      -> em1      -> v4: 10.76.0.1/24

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) Update 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: 2
    
```

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 WAN IP address will be 172.30.10.205.

8) Select 24 bits for the subnet mask.

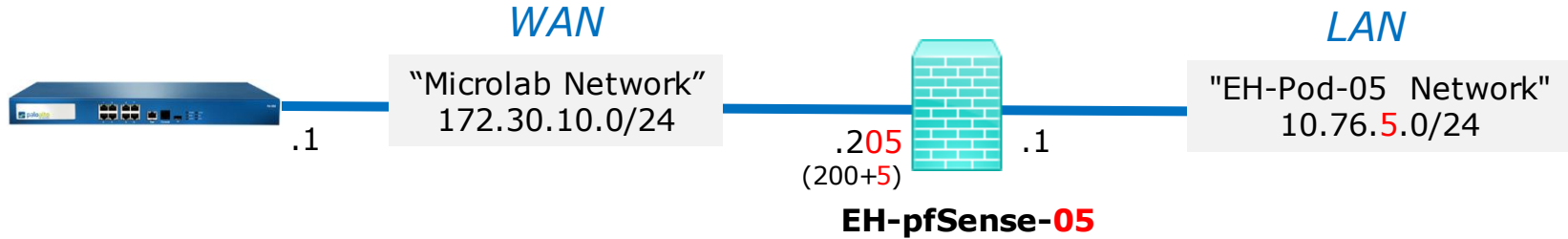
9) Set the upstream gateway to 172.30.10.1.

```

EH-pfSense-05 on 172.30.10.20
File View VM
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.30.10.205
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.30.10.1
Configure IPv6 address WAN interface via DHCP6? (y/n)

```

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



10) Enter "y" to use the DHCP6 for the IPv6 address.

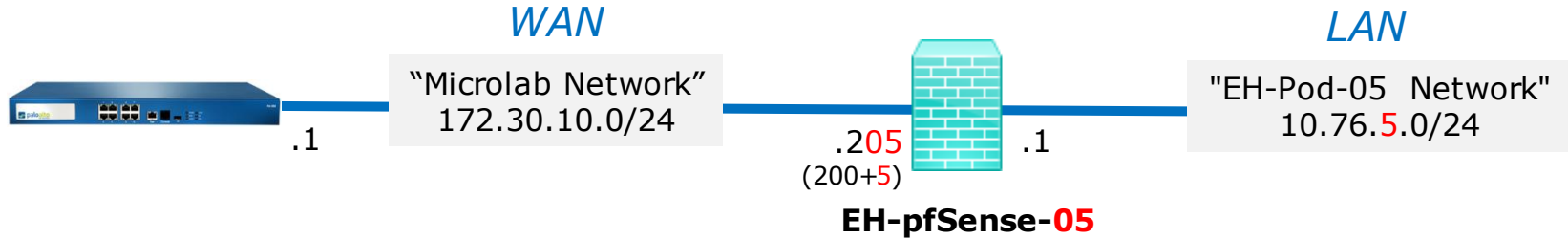
11) Enter "n" to not revert to HTTP as the webConfigurator protocol.

12) Press <ENTER> to continue.

```

EH-pfSense-05 on 172.30.10.20
File View VM
[Icons]
255.255.0.0 = 16
255.0.0.0 = 8
Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.30.10.1
Configure IPv6 address WAN interface via DHCP6? (y/n) y
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 WAN address has been set to 172.30.10.205/24
The IPv6 WAN address has been set to dhcp6
Press <ENTER> to continue.
    
```

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



13) Verify the WAN interface was setup correctly.

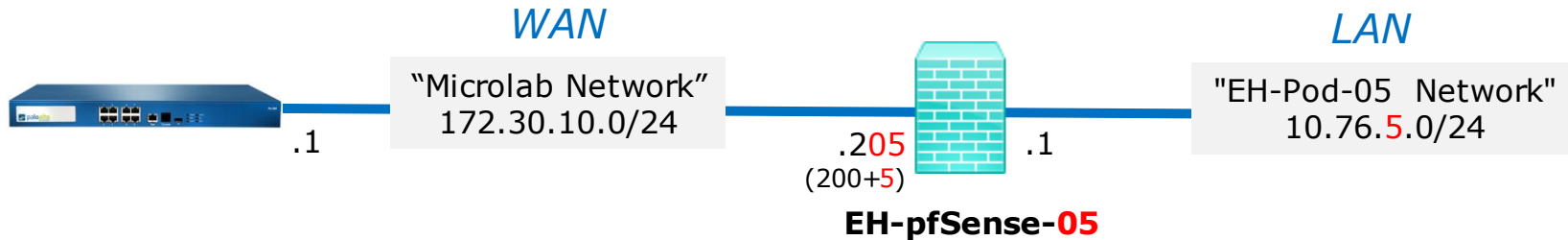
```

EH-pfSense-05 on 172.30.10.20
File View VM
The IPv4 WAN address has been set to 172.30.10.205/24
The IPv6 WAN address has been set to dhcp6
Press <ENTER> to continue.
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***
WAN (wan)      -> em0      -> v4: 172.30.10.205/24
                v6/DHCP6: 2607:f380:80f:f427:250:56ff:feaf:b80
LAN (lan)      -> em1      -> v4: 10.76.0.1/24

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) Update 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: █
    
```

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.

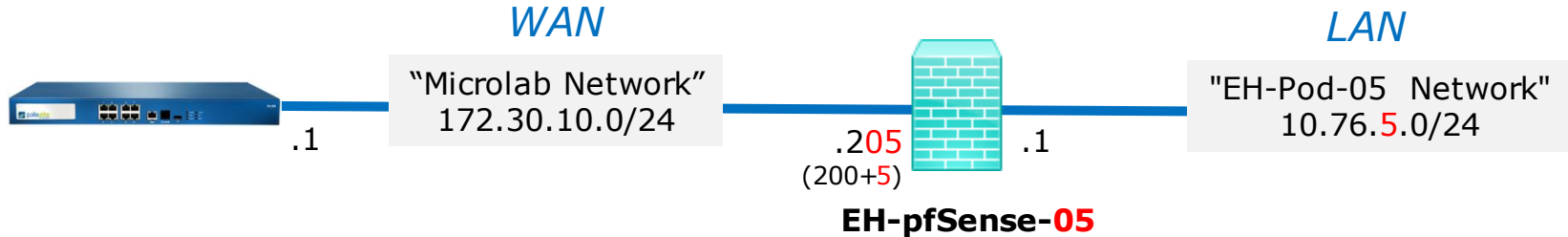
17) Select 24 bits for the subnet mask.

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

```

EH-pfSense-05 on 172.30.10.20
File View VM
Enter an option: 2
Available interfaces:
1 - WAN (em0 - static, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.76.5.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
    
```


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.

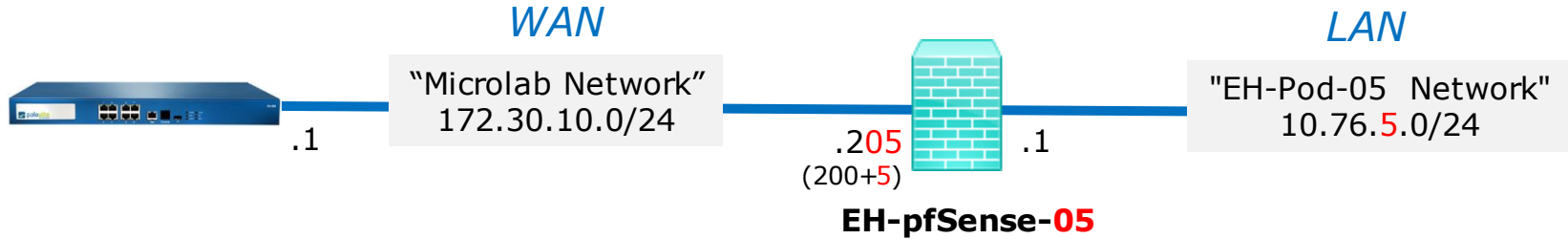
21) Enter "n" to not revert to HTTP for the webConfigurator. We will be using HTTPS.

22) Press <ENTER> to continue.

```

EH-pfSense-05 on 172.30.10.20
File View VM
[Icons]
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new LAN IPv6 address. Press <ENTER> for none:
> 
Do you want to enable the DHCP server on LAN? (y/n)  n
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n)  n
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 LAN address has been set to 10.76.5.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.76.5.1/
Press <ENTER> to continue.
To release cursor, press CTRL + ALT
    
```

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



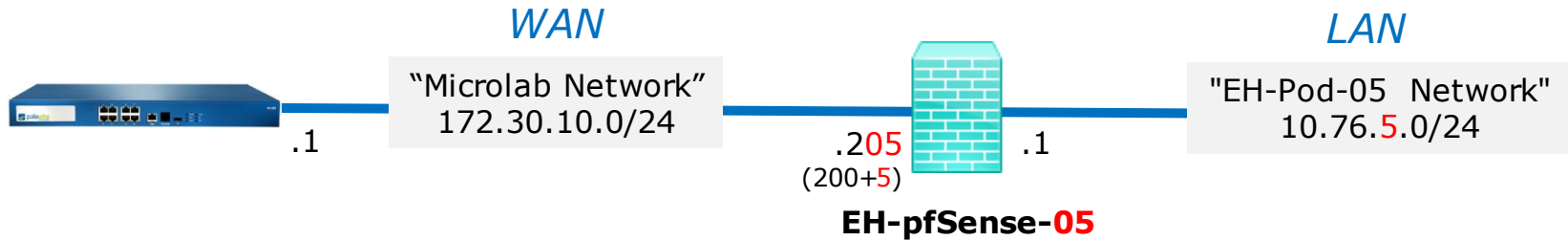
23) Verify the IP address on your LAN interface. The third octet should be your pod number.

```

EH-pfSense-05 on 172.30.10.20
File View VM
The IPv4 LAN address has been set to 10.76.5.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
https://10.76.5.1/
Press <ENTER> to continue.
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***
WAN (wan)      -> em0      -> v4: 172.30.10.205/24
                v6/DHCP6: 2607:f380:80f:f427:250:56ff:feaf:b80
9/64
LAN (lan)      -> em1      -> v4: 10.76.5.1/24
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) Update 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: █
To release cursor, press CTRL + ALT
    
```

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

```

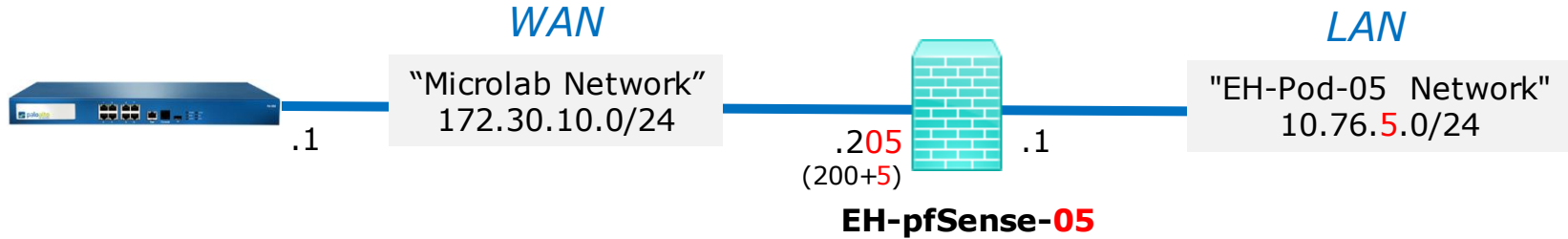
EH-pfSense-05 on 172.30.10.20
File View VM
[Icons]
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: 8

[2.3.1-RELEASE][root@EH-pfSense-xx.cis.cabrillo.edu]/root: ping -c4 google.com
PING google.com (216.58.195.238): 56 data bytes
64 bytes from 216.58.195.238: icmp_seq=0 ttl=57 time=3.643 ms
64 bytes from 216.58.195.238: icmp_seq=1 ttl=57 time=3.846 ms
64 bytes from 216.58.195.238: icmp_seq=2 ttl=57 time=3.917 ms
64 bytes from 216.58.195.238: icmp_seq=3 ttl=57 time=3.926 ms

--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.643/3.833/3.926/0.114 ms
[2.3.1-RELEASE][root@EH-pfSense-xx.cis.cabrillo.edu]/root:
    
```

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.

```

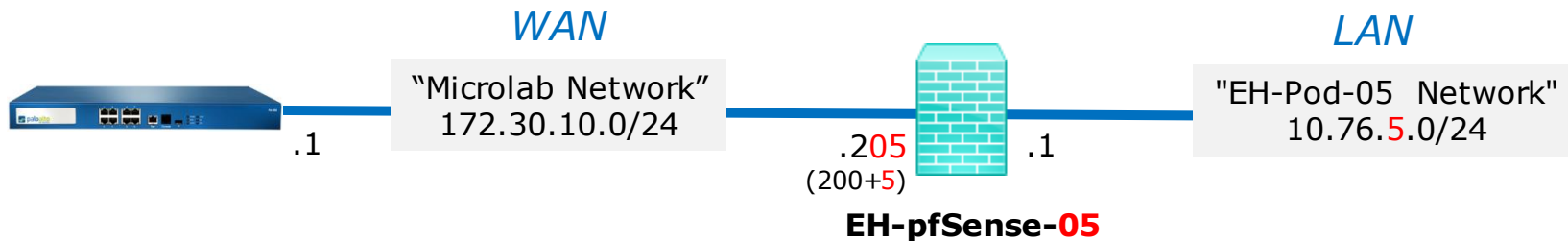
EH-pfSense-05 on
File View VM
--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.764/4.862/4.906/0.057 ms
[2.3.1-RELEASE][root@EH-pfSense-xx.cis.cabrillo.edu]/root: exit
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***

WAN (wan)      -> em0      -> v4: 172.30.10.205/24
                v6/DHCP6: 2607:f380:80f:f427:250:56ff:feaf:b80
9/64
LAN (lan)      -> em1      -> v4: 10.76.5.1/24

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) Update 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: 6
  
```

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



27) Type **y** to proceed.

```

EH-pfSense-05 on
File View VM
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***

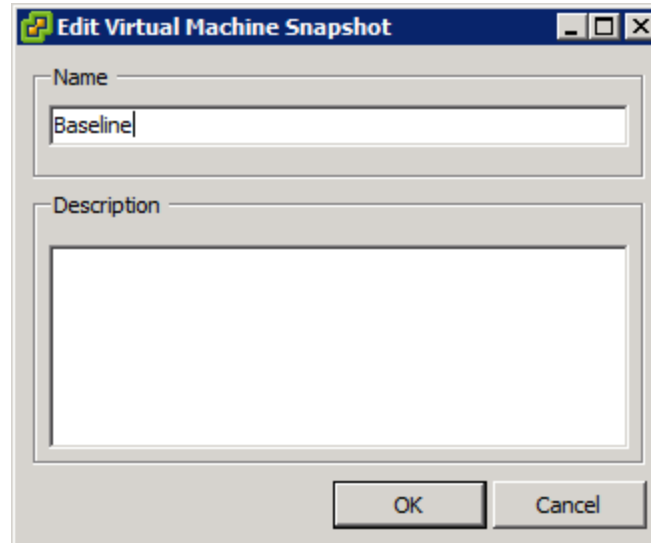
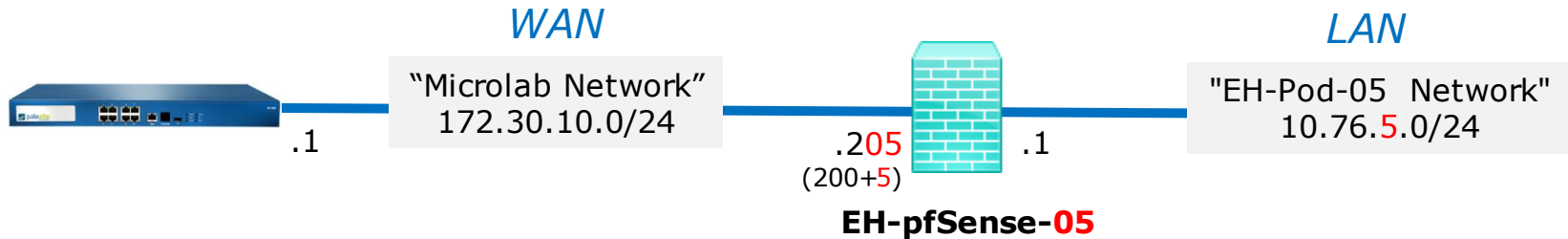
WAN (wan)      -> em0      -> v4: 172.30.10.205/24
                v6/DHCP6: 2607:f380:80f:f427:250:56ff:feaf:b80
9/64
LAN (lan)      -> em1      -> v4: 10.76.5.1/24

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) Update 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: 6

pfSense will shutdown and halt system. This may take a few minutes, depending on
your hardware.
Do you want to proceed [y|n]? y
To release cursor, press CTRL + ALT
    
```

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

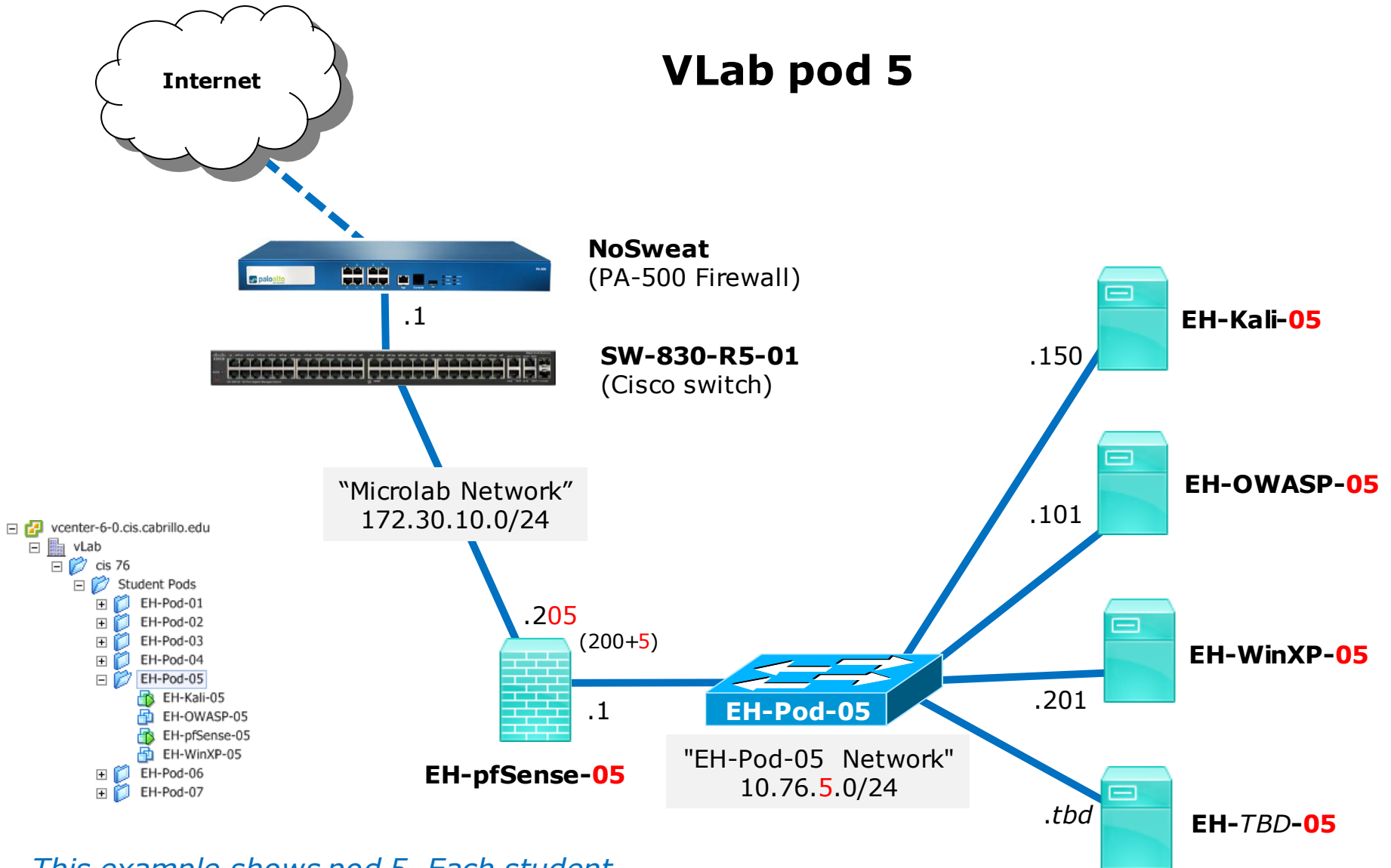


Save your work

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

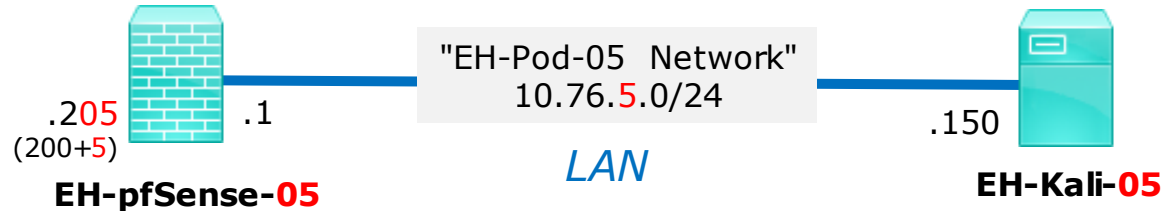
Kali VM Config

VLab pod 5



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

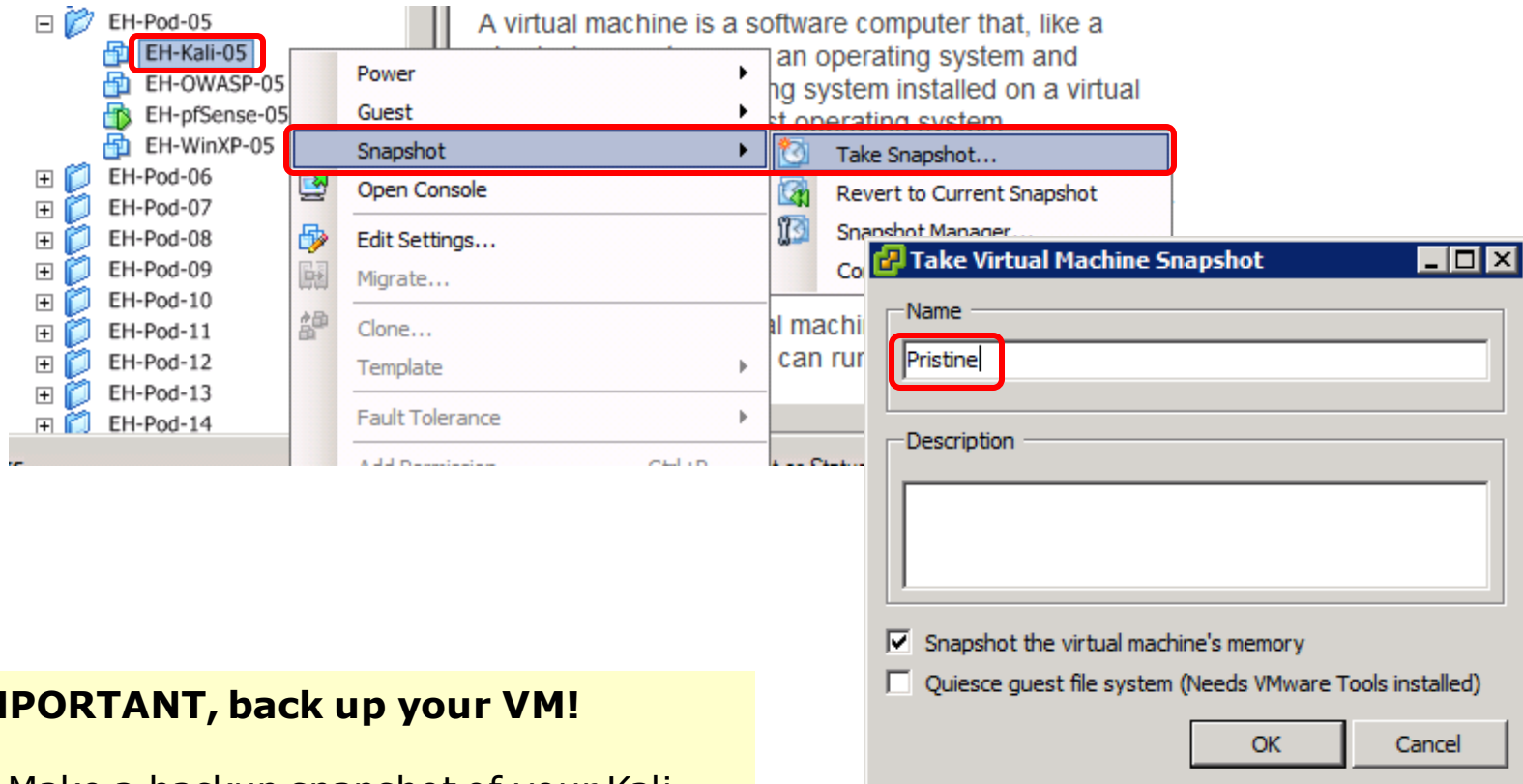


This example shows pod 5.

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

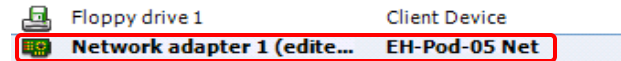
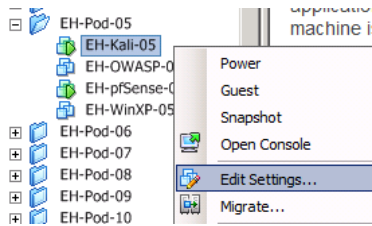
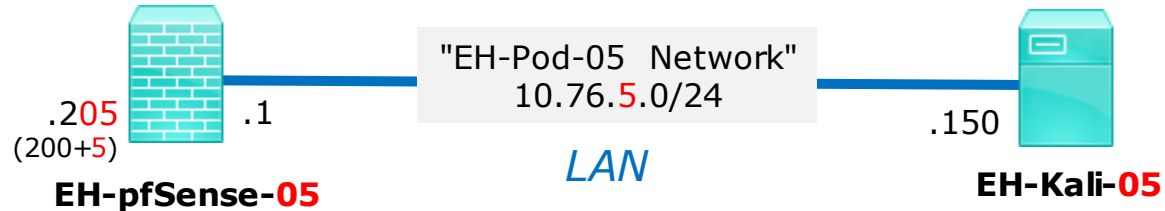
Example: Configuring the EH-Kali VM in EH-Pod-05



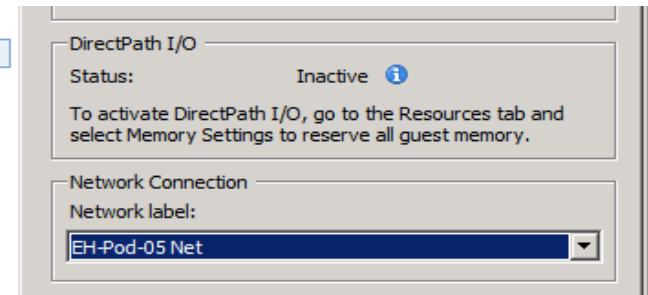
IMPORTANT, back up your VM!

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

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



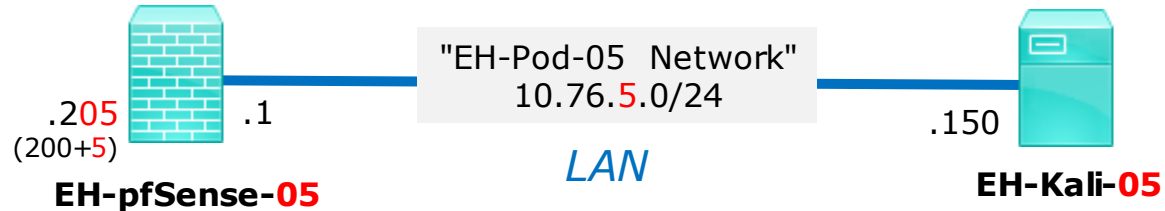
*This example shows pod 5.
Each student should only use
the pod assigned to them.*



Network Cabling

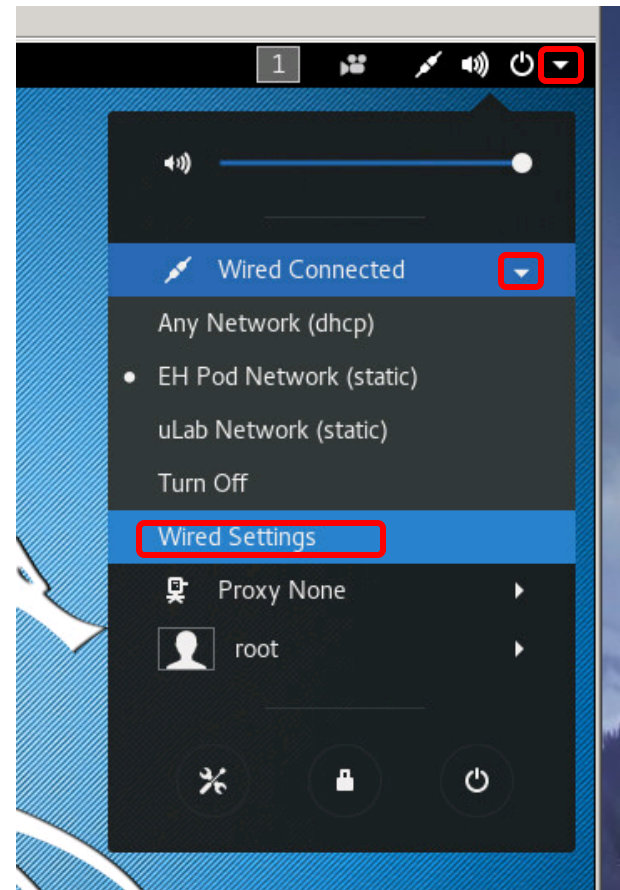
- 1) Edit the settings of your Kali VM.
- 2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

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

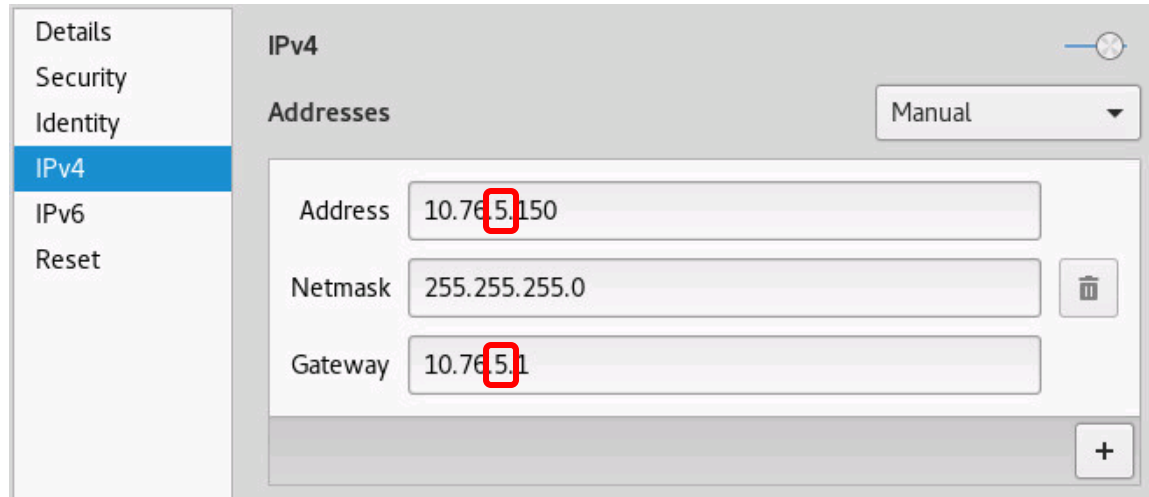
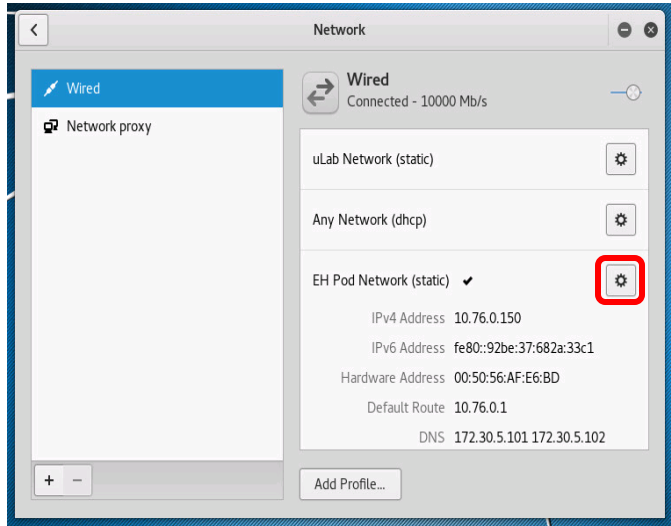
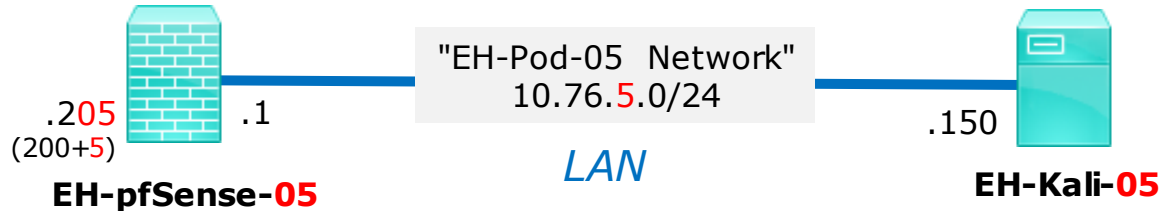


Network Configuration

- 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

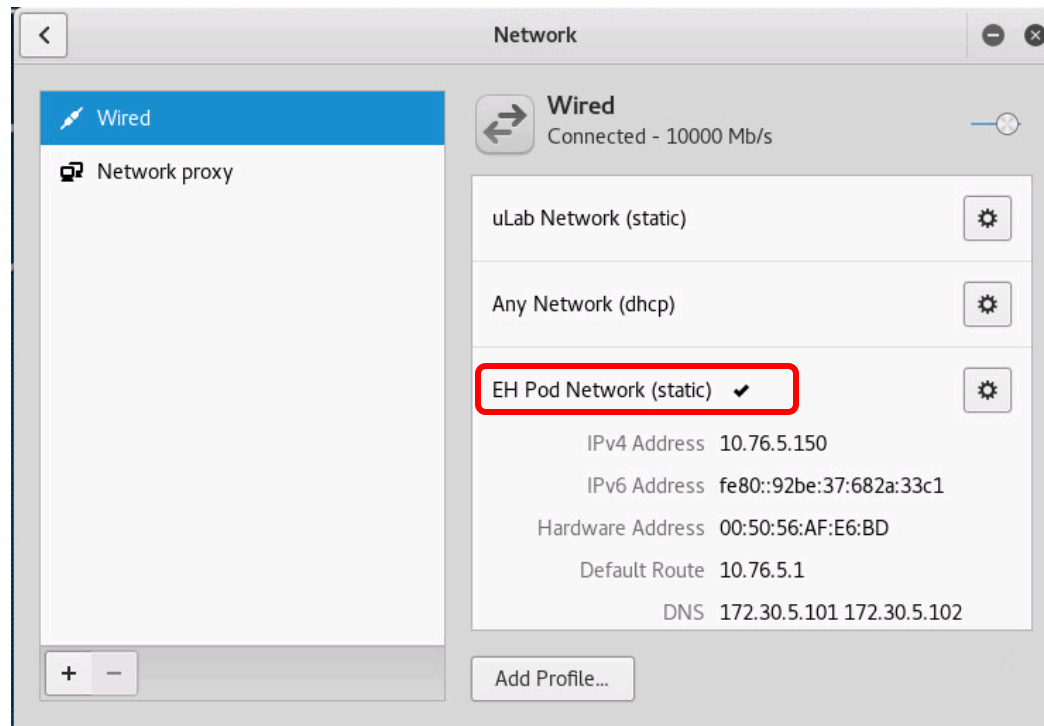
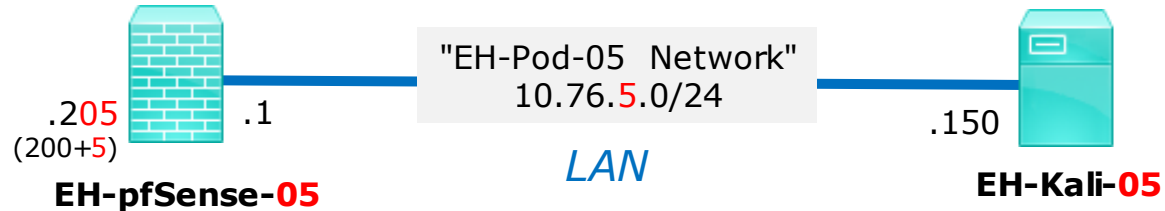


This example shows pod 5. Each student should only use the pod assigned to them.

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

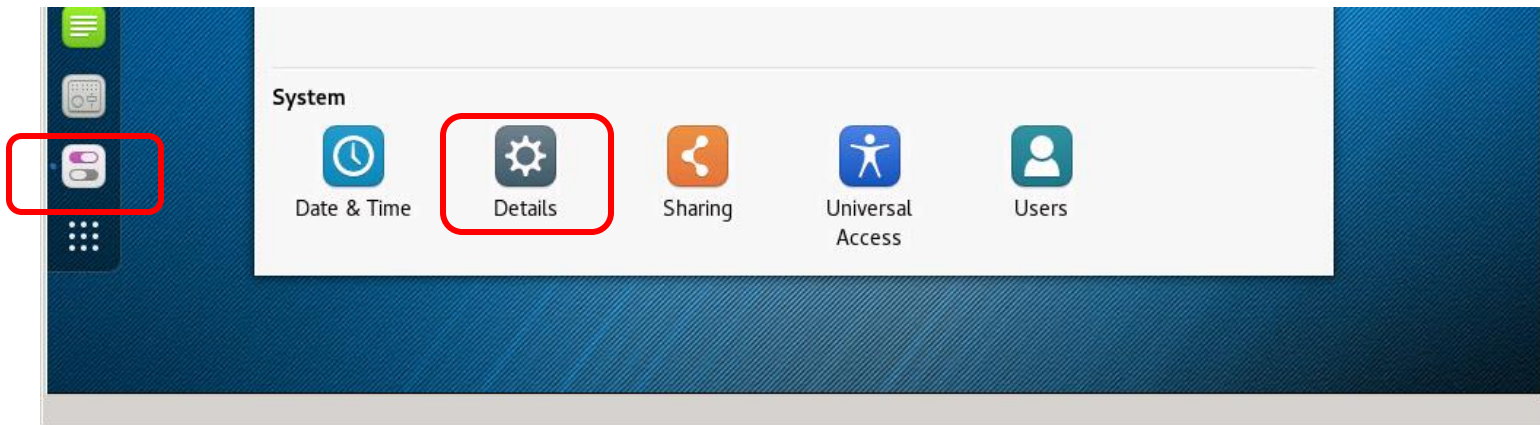
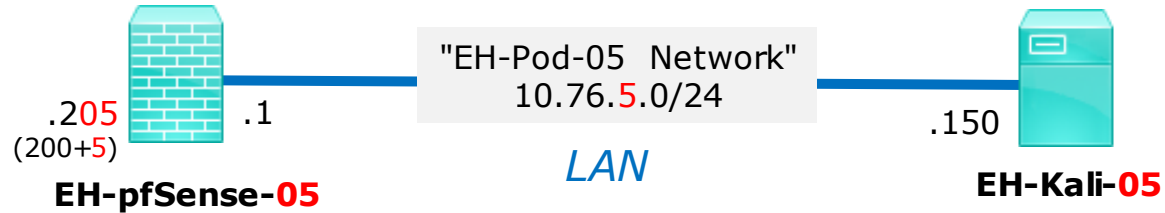
5) Then on the IPv4 tab update the Address and Gateway so the third octet matches your pod number.

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



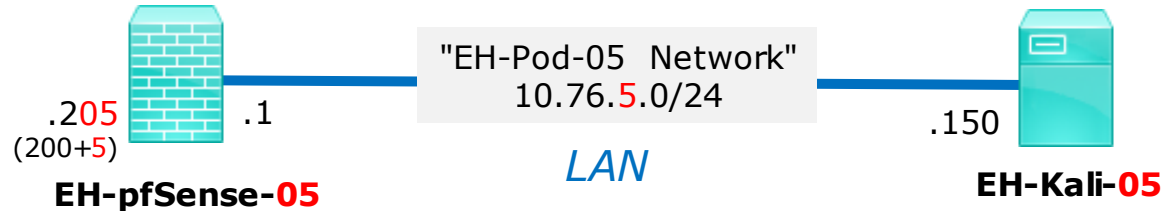
6) Click on the EH Pod Network (static) profile and make sure you see the updated IPv4 address and Default Route. Then close the Network dialog box.

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



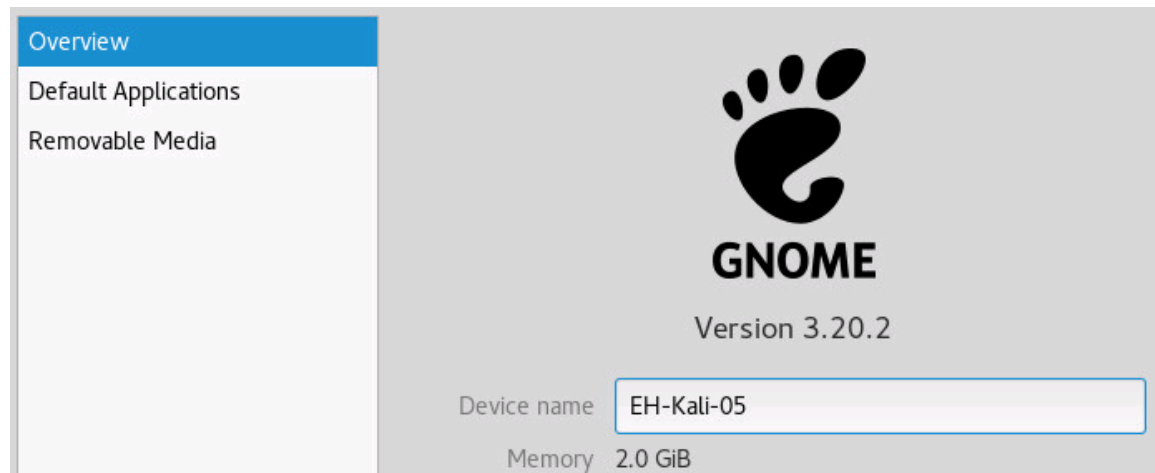
7) Click the Settings icon on the left panel then the Details icon on the All Settings dialog box.

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



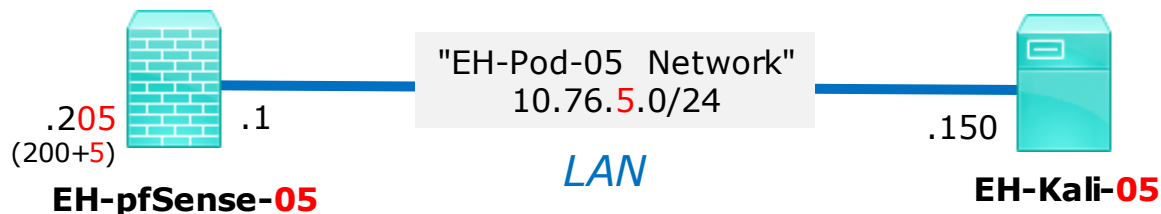
This example shows pod 5.

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 opus.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

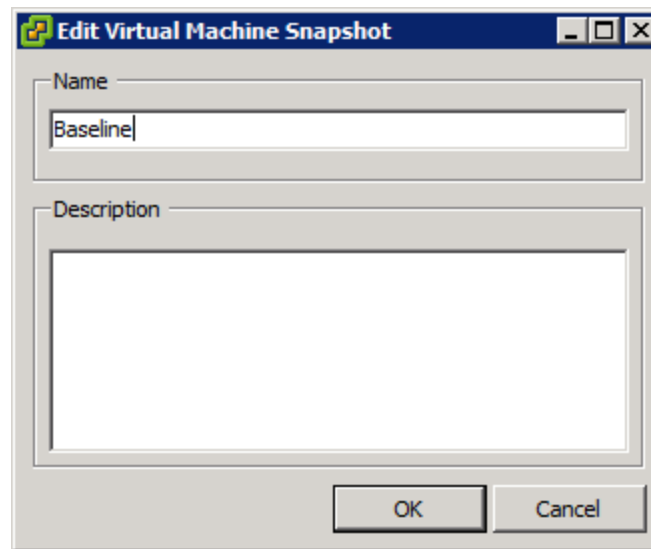
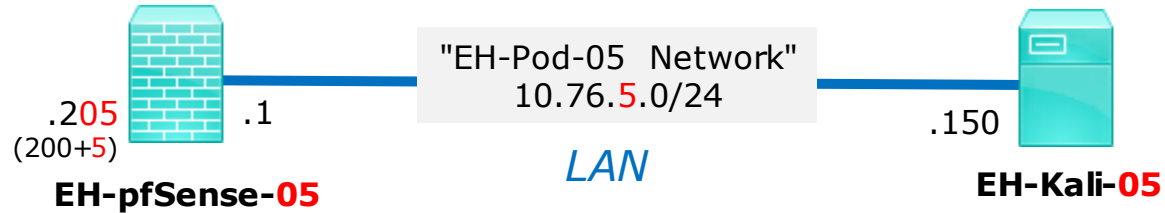
--- oslab.cis.cabrillo.edu ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.879/1.060/1.242/0.184 ms
root@eh-kali-05:~# ping google.com -c2
PING google.com (216.58.194.174) 56(84) bytes of data.
64 bytes from sfo07s13-in-f14.1e100.net (216.58.194.174):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

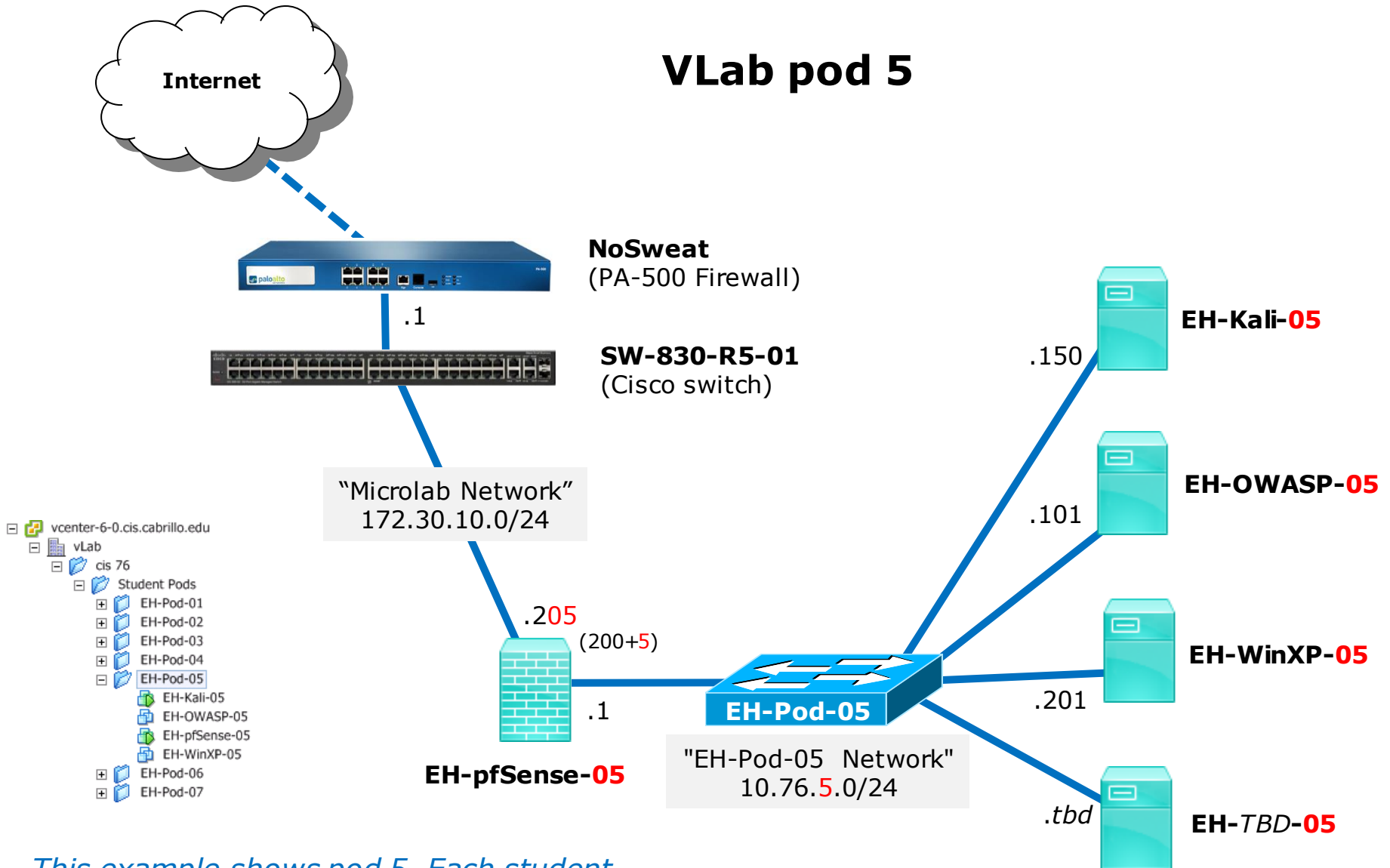


Save your work

Shutdown VM and make a second snapshot named Baseline

WinXP VM Config

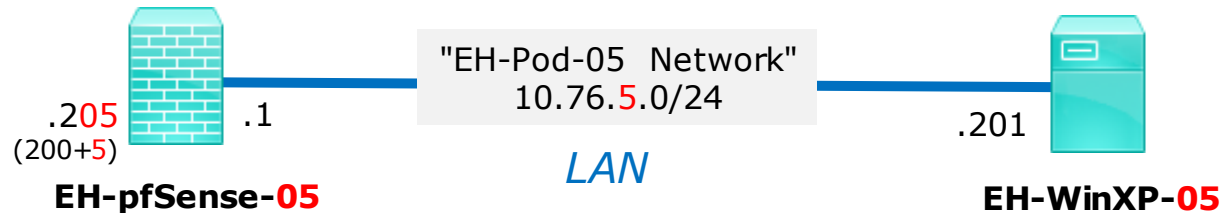
VLab pod 5



- vcen-6-0.cis.cabrillo.edu
 - vLab
 - cis 76
 - Student Pods
 - EH-Pod-01
 - EH-Pod-02
 - EH-Pod-03
 - EH-Pod-04
 - EH-Pod-05
 - EH-Kali-05
 - EH-OWASP-05
 - EH-pfSense-05
 - EH-WinXP-05
 - EH-Pod-06
 - EH-Pod-07

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

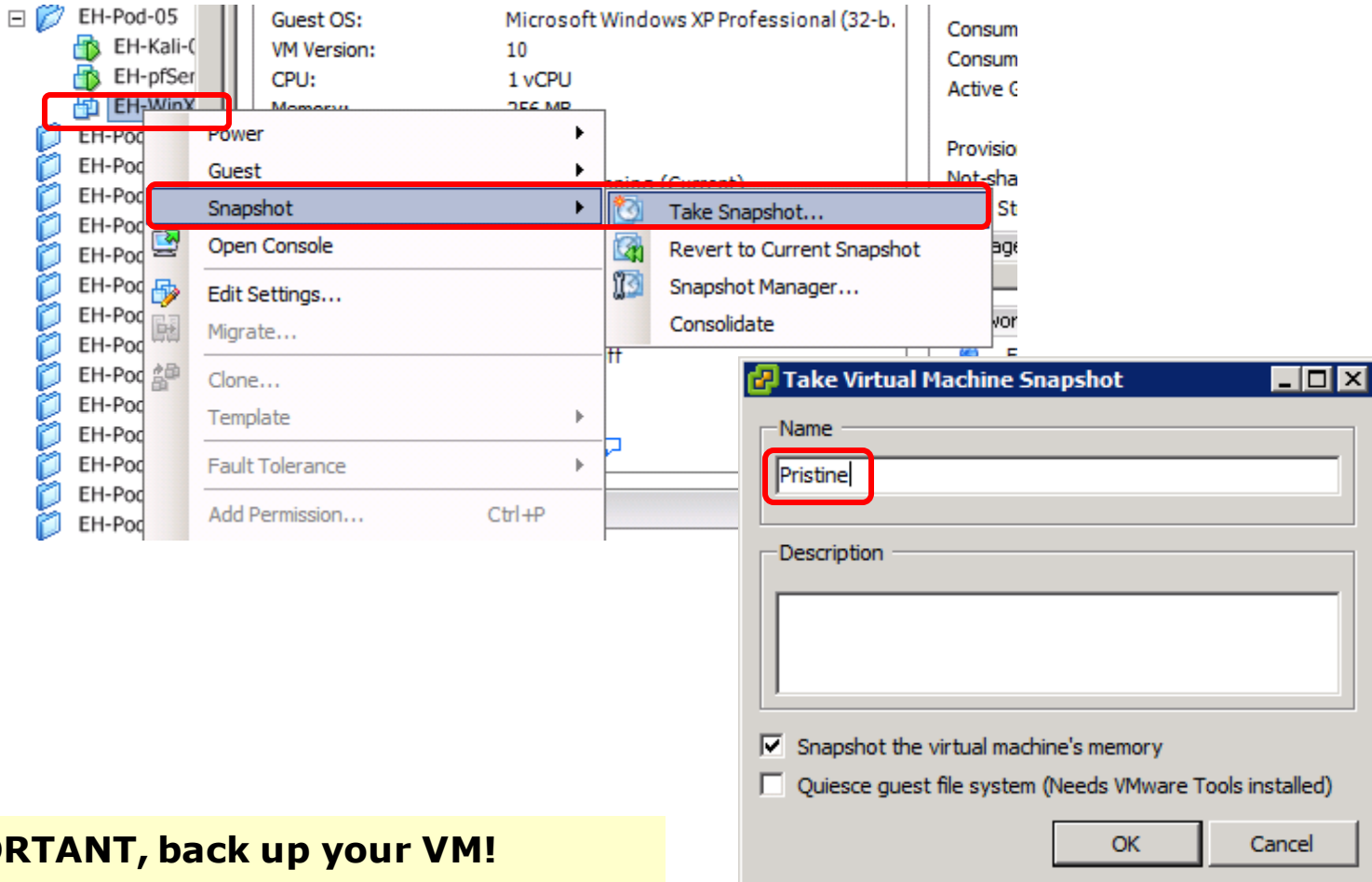


This example shows pod 5.

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

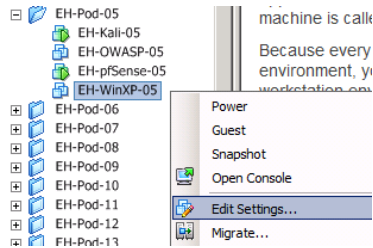
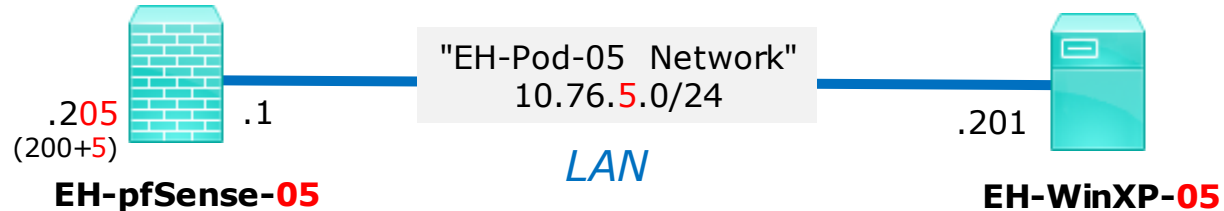
Example: Configuring the EH-WinXP VM in EH-Pod-05



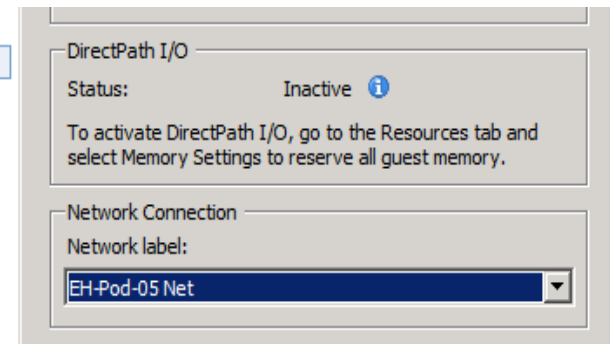
IMPORTANT, back up your VM!

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

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



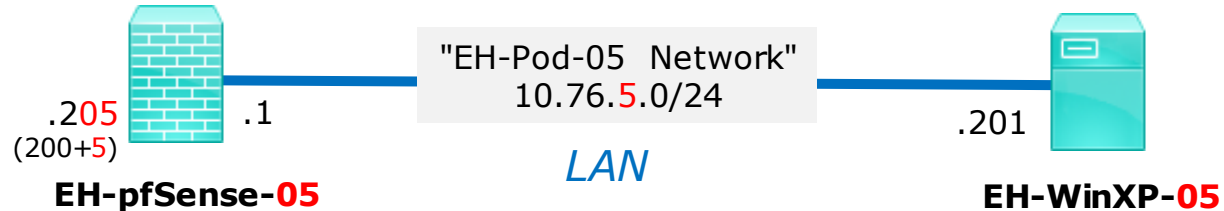
*This example shows pod 5.
Each student should only use
the pod assigned to them.*



Network Cabling

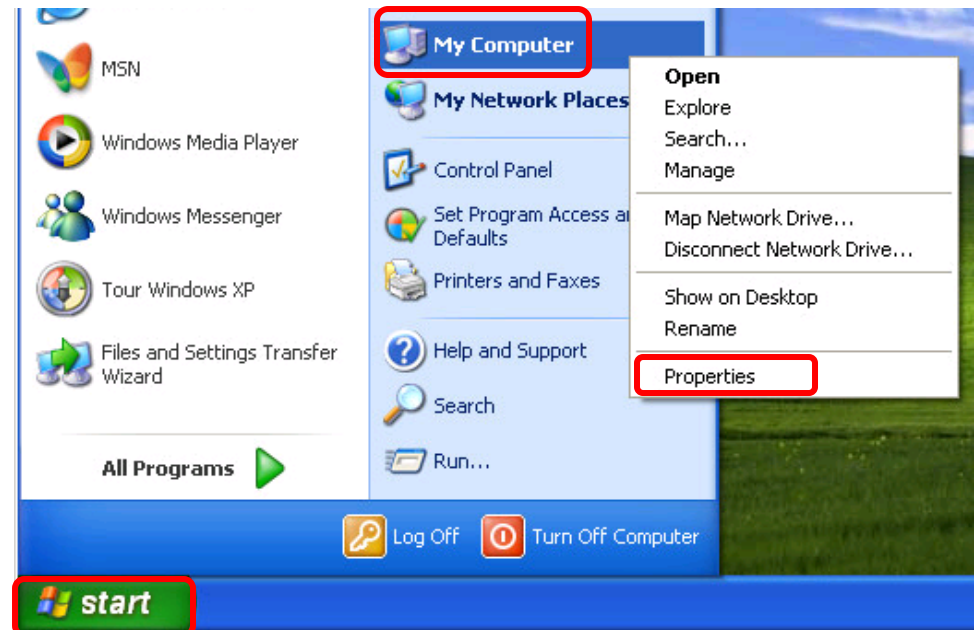
- 1) Edit the settings of your WinXP VM.
- 2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

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

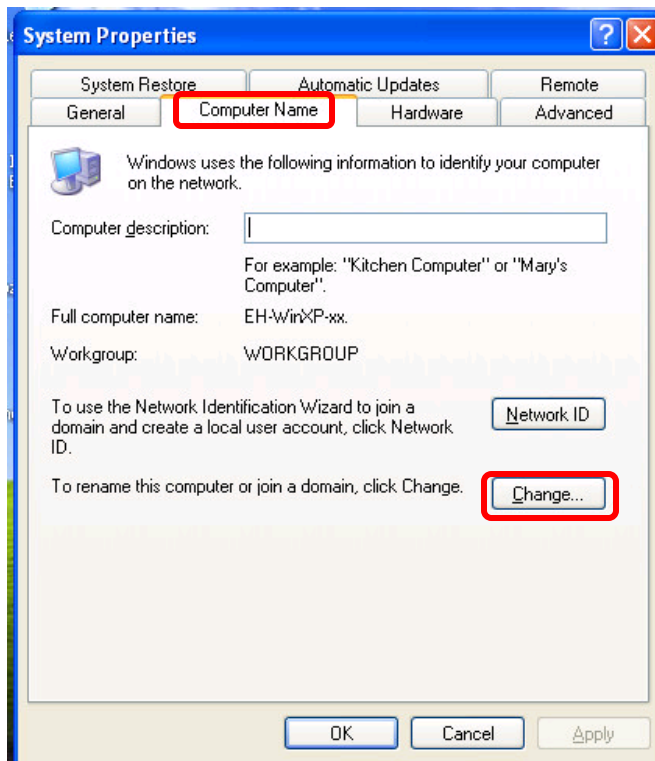
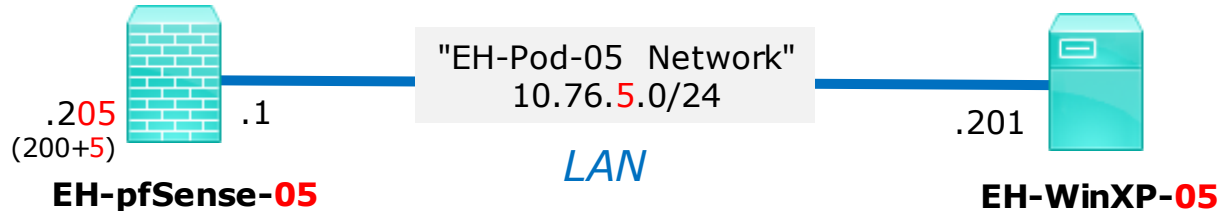


Computer Name Configuration

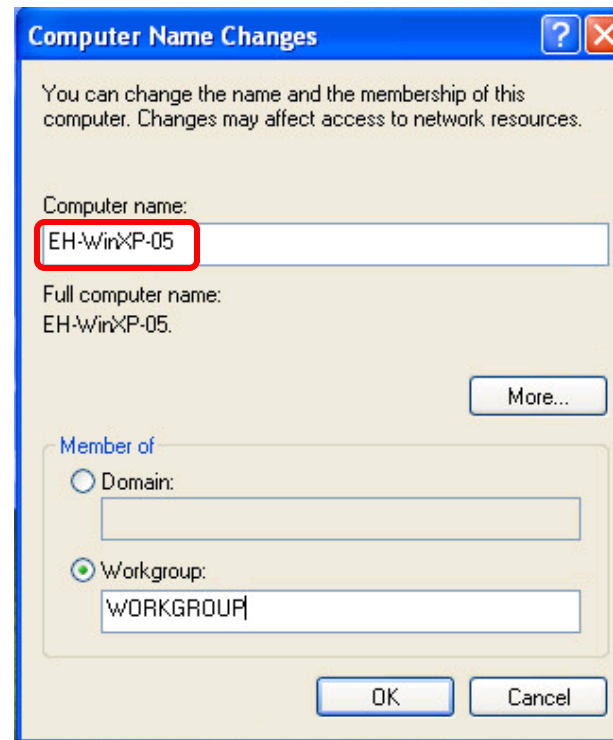
- 1) Power up the VM and open a console.
- 2) Login as the cis76 student user.
- 3) Click Start, right-click on My Computer and Select Properties.



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

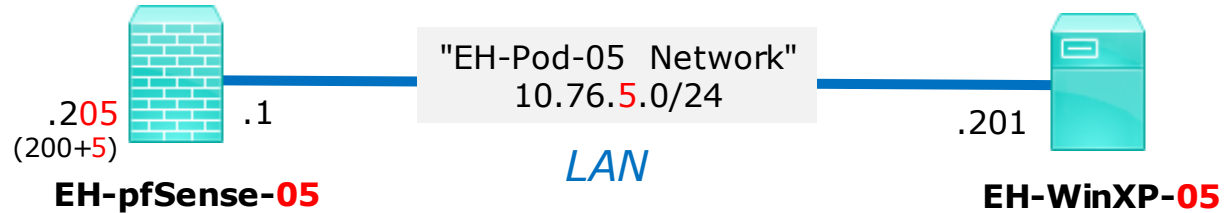


4) Click the Computer Name tab then click Change.



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

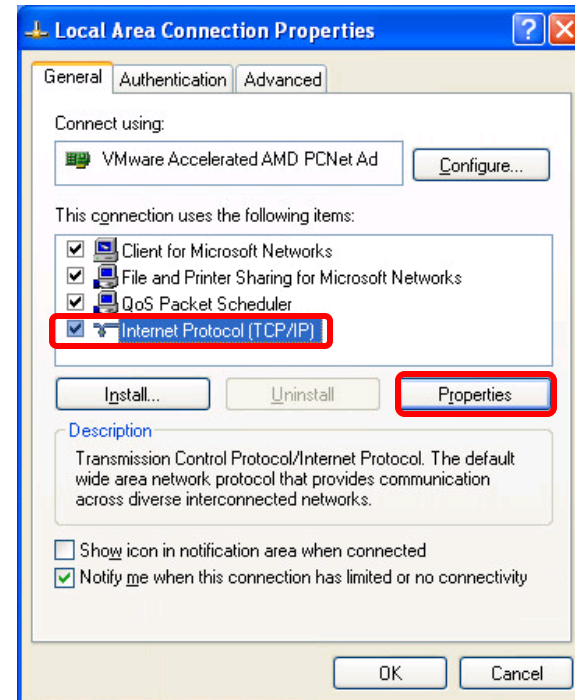
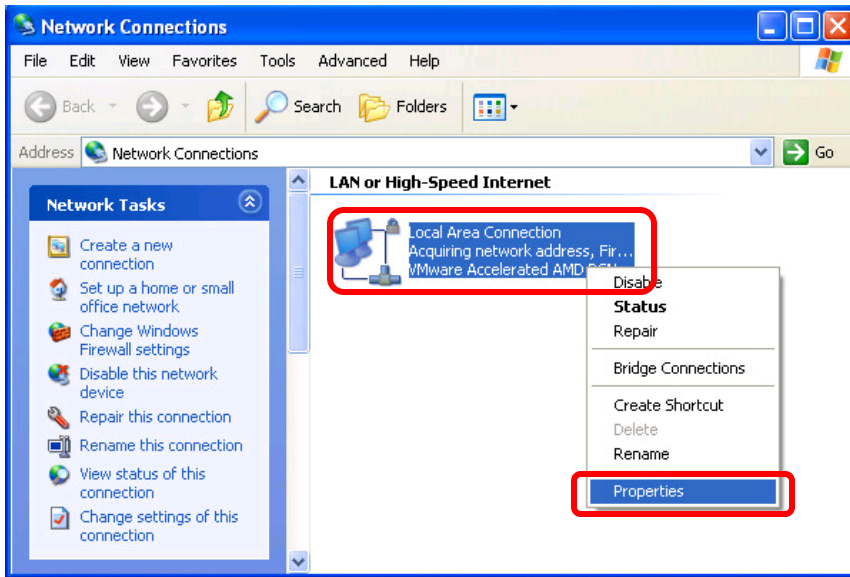
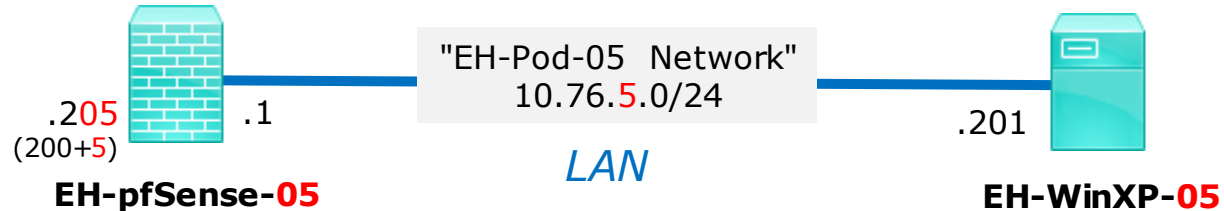


Network Configuration

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



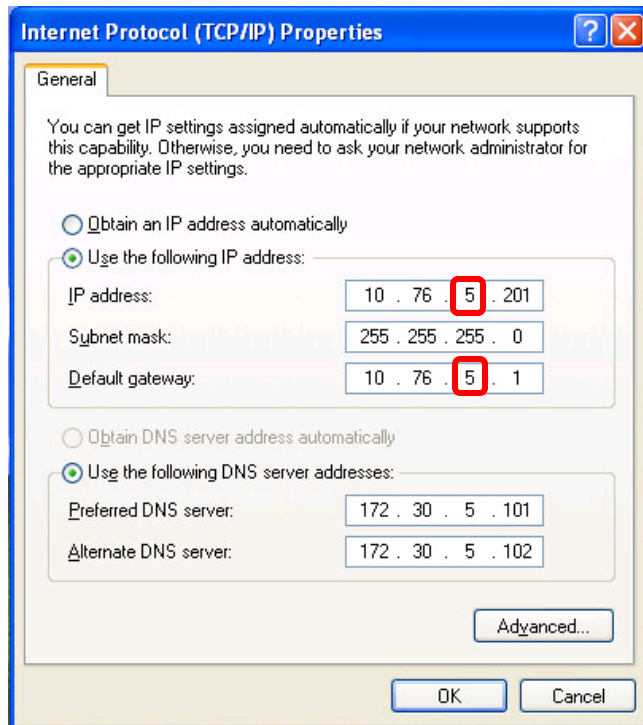
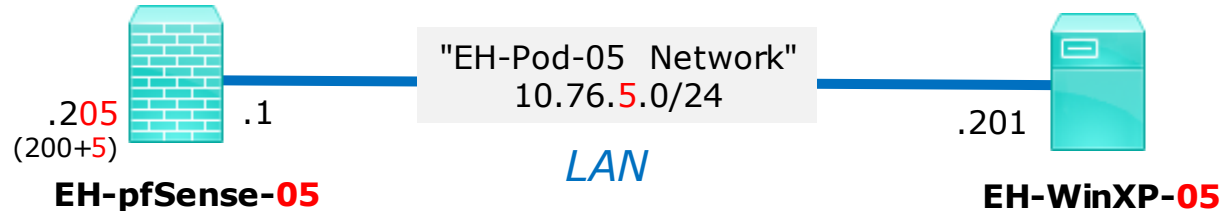
Example: Configuring the EH-WinXP VM in EH-Pod-05



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

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

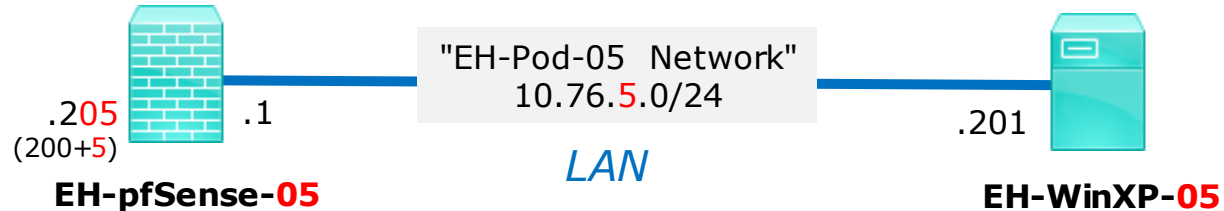
Example: Configuring the EH-WinXP VM in EH-Pod-05



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



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>ping google.com

Pinging google.com [216.58.194.174] with 32 bytes of data:

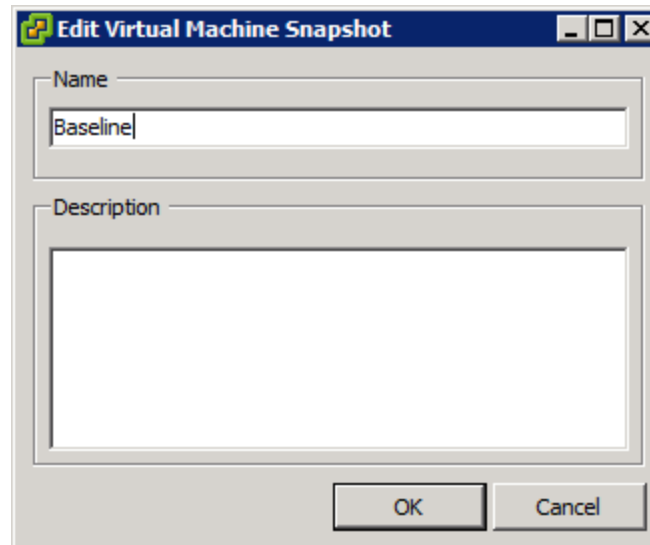
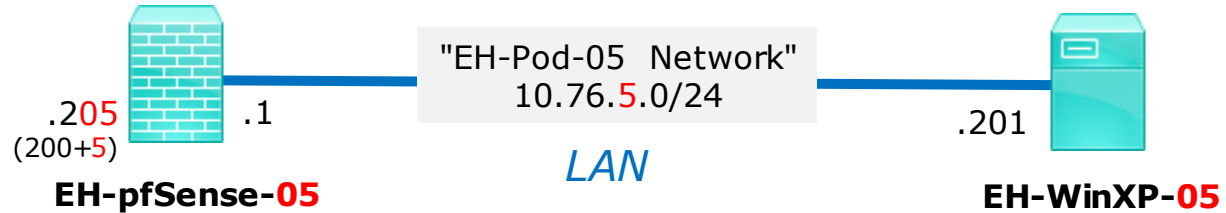
Reply from 216.58.194.174: bytes=32 time=4ms TTL=56
Reply from 216.58.194.174: bytes=32 time=4ms TTL=56
Reply from 216.58.194.174: bytes=32 time=4ms TTL=56
Reply from 216.58.194.174: bytes=32 time=4ms TTL=56

Ping statistics for 216.58.194.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Documents and Settings\cis76 student>
    
```

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

The screenshot shows the pfSense web interface for editing a NAT Port Forward rule. The browser address bar shows the URL `https://10.76.5.1/firewall_nat_edit.php?id=0`. The page title is "Firewall / NAT / Port Forward / Edit".

The configuration form includes the following fields:

- Disabled:** Disable this rule
- No RDR (NOT):** Disable redirection for traffic matching this rule. This option is rarely needed. Don't use this without thorough knowledge of the implications.
- Interface:** WAN
- Protocol:** TCP
- Source:** [Display Advanced](#)
- Destination:** Invert match. WAN address (Type: Address/mask)
- Destination port range:** SSH (From port: Custom, To port: Custom). Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
- Redirect target IP:** 10.76.5.150. Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12
- Redirect target port:** SSH

This example is for Pod 5

Forward SSH through pfSense Firewall to Kali

The screenshot shows the pfSense Firewall configuration interface in a web browser. The page is titled "Firewall: NAT: Port Forward: Edit" and is for a rule named "Rule NAT Forward ssh to kali". The configuration is as follows:

- Redirect target IP:** 10.76.5.150
- Redirect target port:** SSH
- Description:** Forward ssh to kali
- No XMLRPC Sync:** Do not automatically sync to other CARP members
- NAT reflection:** Use system default
- Filter rule association:** Rule NAT Forward ssh to kali

Rule Information

Created	8/23/16 17:12:41 by admin@10.76.5.150
Updated	8/23/16 17:12:41 by admin@10.76.5.150

A "Save" button is visible at the bottom of the configuration form.

Zoom in to see settings

Forward SSH through pfSense Firewall to Kali

EH-Kali-05 on

Applications ▾ Places ▾ Firefox ESR ▾ Tue 17:27

EH-pfSense-05.cis.cabrillo.edu - Firewall: NAT: Port Forward - Mozilla Firefox

Kali Linux, an Offensive S... x EH-pfSense-05.cis.ca... x

https://10.76.5.1/firewall_nat.php

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Sen e COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Firewall / NAT / Port Forward

The changes have been applied successfully.
[Monitor the filter reload progress.](#)

Port Forward 1:1 Outbound NPT

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	10.76.5.150	22 (SSH)	Forward ssh to kali	Edit Delete

Legend
▶ Pass
🔗 Linked rule

pfSense is © 2004 - 2016 by Electric Sheep Fencing LLC. All Rights Reserved. [view license](#)

Don't forget to save your changes and apply them

Forward SSH through pfSense Firewall to Kali

```

EH-Kali-05 on
File View VM
Applications Places Terminal Tue 17:23
root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# service sshd start
root@eh-kali-05:~# ps -ef | grep ssh
root    1134  1064  0 12:45 ?        00:00:00 /usr/bin/ssh-agent x-session-man
ager
root    3857      1  0 17:22 ?        00:00:00 /usr/sbin/sshd -D
root    3859  3718  0 17:22 pts/0    00:00:00 grep ssh
root@eh-kali-05:~# service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disa
   Active: active (running) since Tue 2016-08-23 17:22:46 PDT; 12s ago
   Main PID: 3857 (sshd)
   CGroup: /system.slice/ssh.service
           └─3857 /usr/sbin/sshd -D

Aug 23 17:22:46 eh-kali-05 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 23 17:22:46 eh-kali-05 sshd[3857]: Server listening on 0.0.0.0 port 22.
Aug 23 17:22:46 eh-kali-05 sshd[3857]: Server listening on :: port 22.
Aug 23 17:22:46 eh-kali-05 systemd[1]: Started OpenBSD Secure Shell server.
root@eh-kali-05:~#
    
```

Start the ssh serve on Kali

```
cis76@eh-kali-05: ~  
[rsimms@oslab ~]$ nmap -Pn -sT -p22 172.30.10.205  
Starting Nmap 5.51 ( http://nmap.org ) at 2016-08-23 17:30 PDT  
Nmap scan report for 172.30.10.205  
Host is up (0.0013s latency).  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds  
[rsimms@oslab ~]$  
[rsimms@oslab ~]$  
[rsimms@oslab ~]$  
[rsimms@oslab ~]$  
[rsimms@oslab ~]$ ssh cis76@172.30.10.205  
cis76@172.30.10.205's password:  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Tue Aug 23 17:16:39 2016 from 172.30.5.20  
cis76@eh-kali-05:~$ █
```

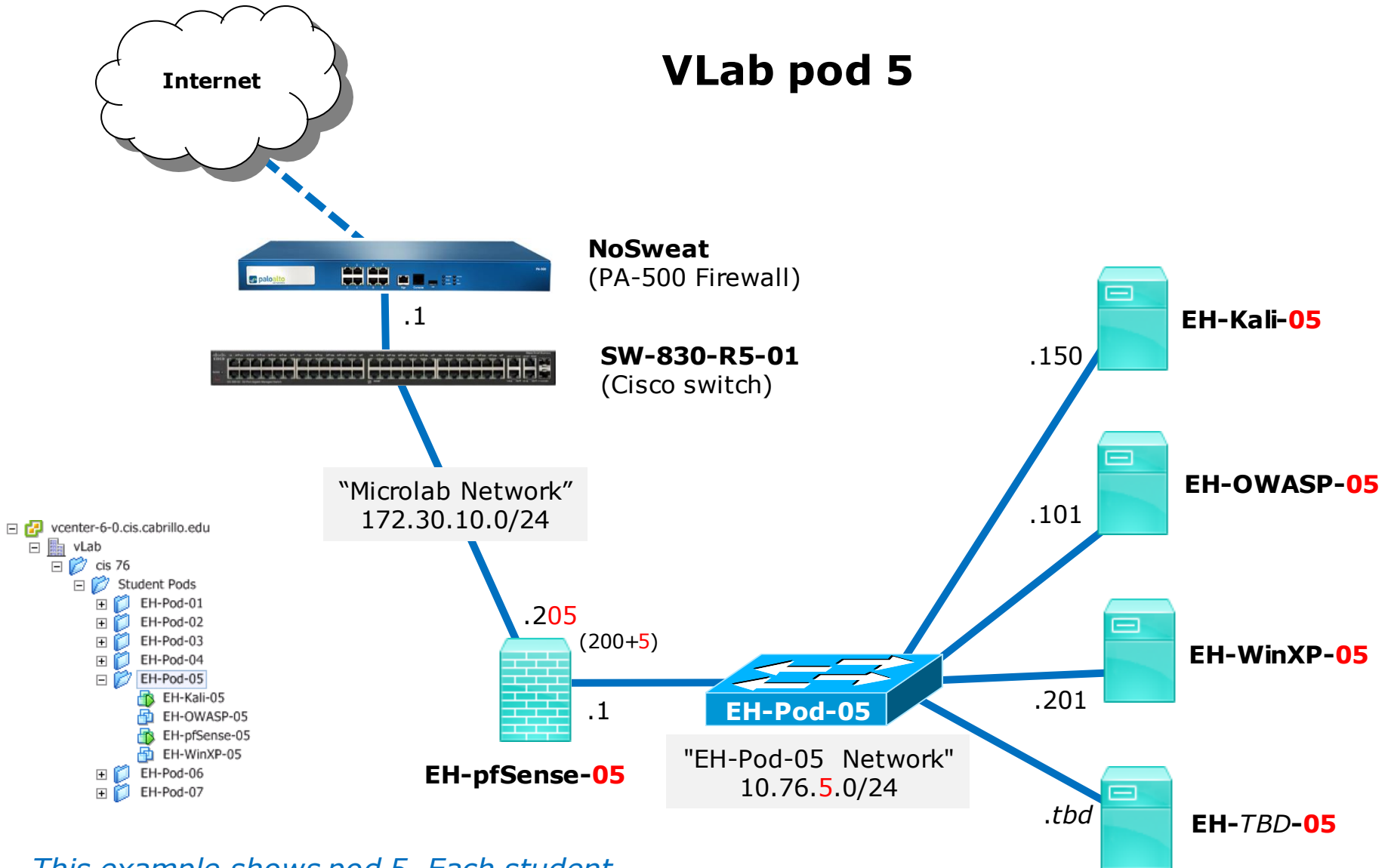
You can now use your favorite terminal emulator and use copy and paste

Work in Progress

- OWASP VM config

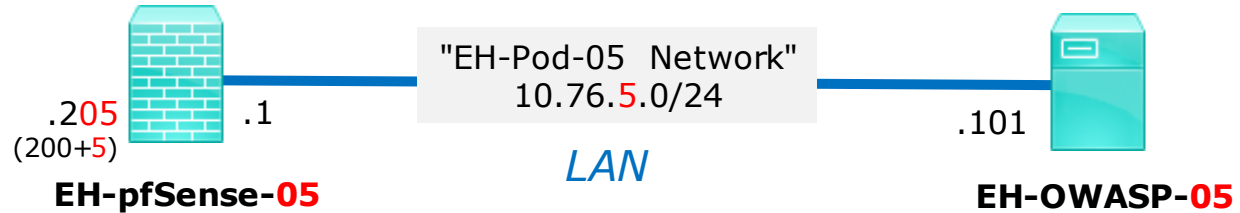
OWASP VM Config

VLab pod 5



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

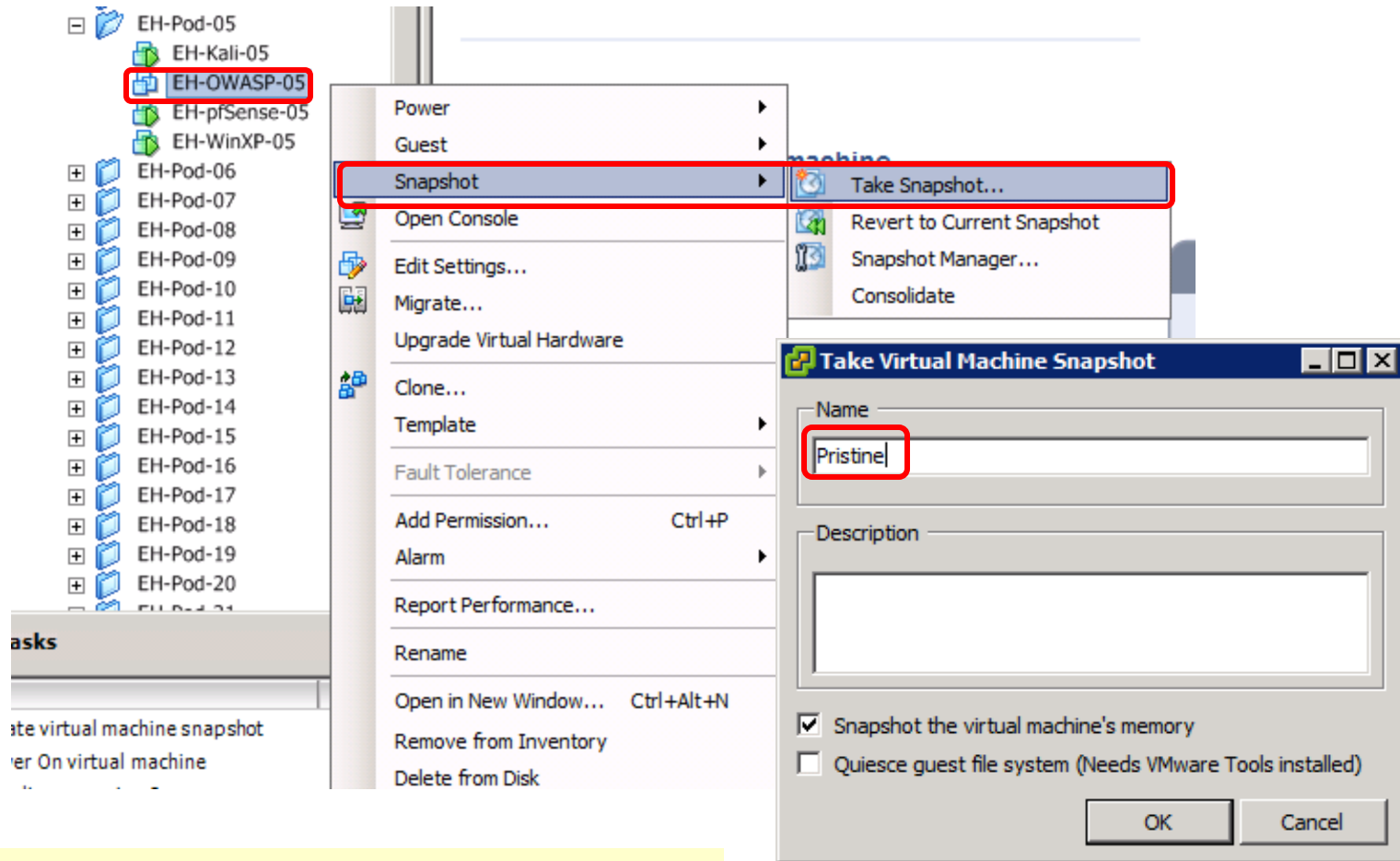


This example shows pod 5.

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

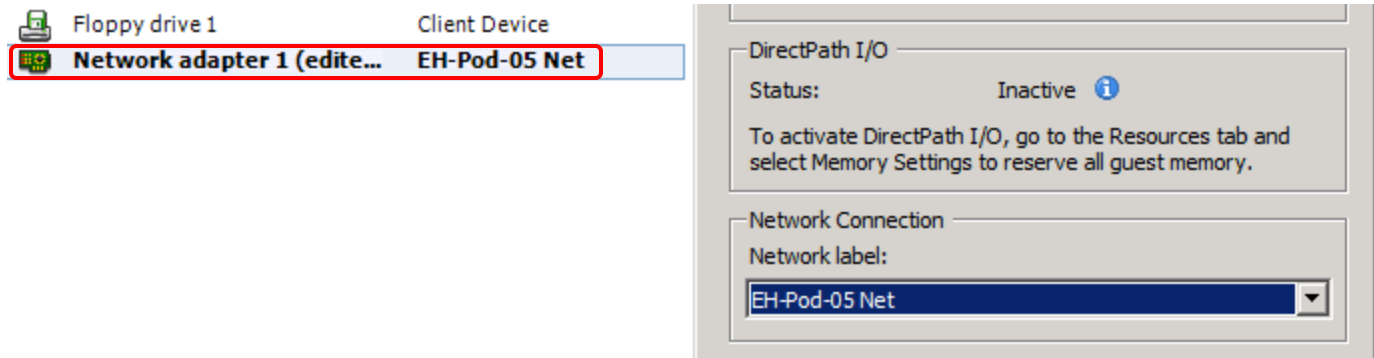
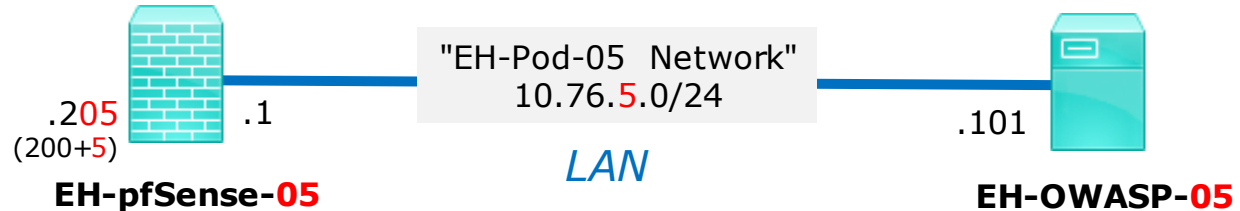
Example: Configuring the EH-OWASP VM in EH-Pod-05



IMPORTANT, back up your VM!

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

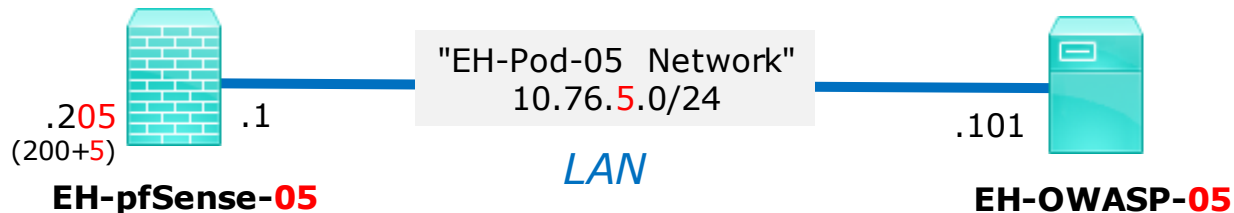
Example: Configuring the EH-OWASP VM in EH-Pod-05



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.
 - b) Add: **dns-search cis.cabrillo.edu**
 - c) Add: **dns-nameservers 172.30.5.101 172.30.5.102**
 - d) Save and exit.

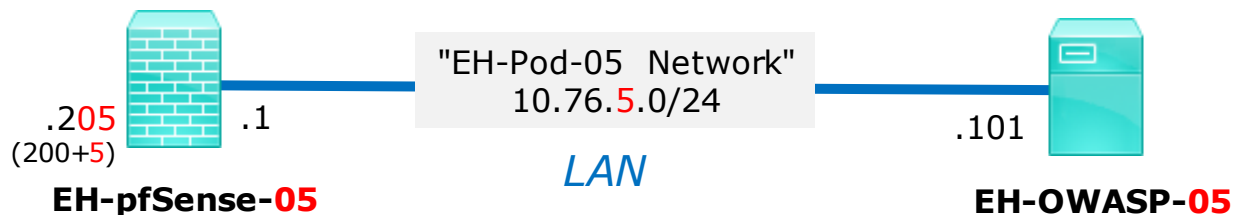
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# 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
```

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.

```

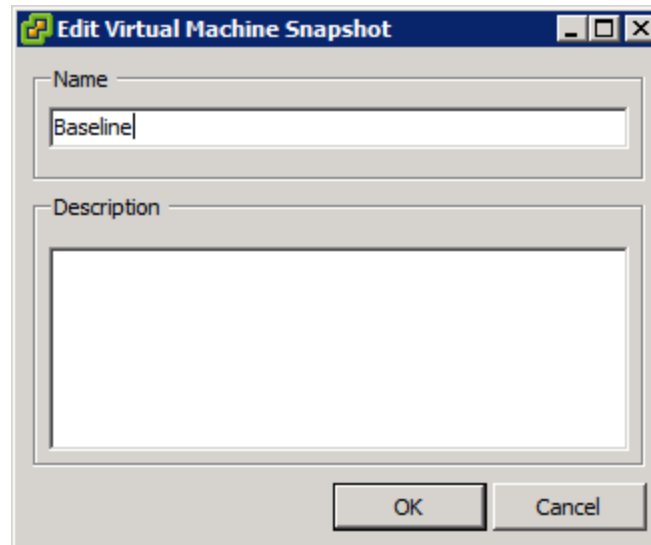
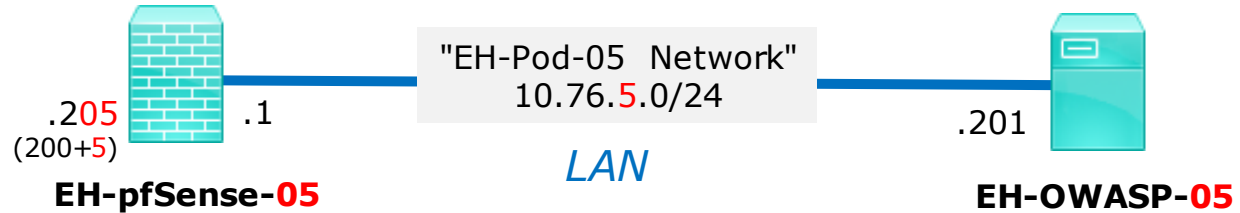
root@owaspbwa:~# /etc/init.d/networking restart
* Reconfiguring network interfaces...
ssh stop/waiting
ssh start/running, process 2231

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 time=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