CIS 76 VLab Pod Setup

Last updated 9/4/2017

Status on setup instructions:

1. pfSense (2.3.1, 64 bit) pfSense-CE-2.3.4-RELEASE-amd64 - DONE for Fa17
2. Kali (2017.1, 64 bit) kali-linux-2017.1-amd64.iso - DONE for Fa17
3. Windows XP (SP2, 32 bit) - DONE for Fa17
4. OWASP_Broken_Web_Apps_VM_1.2 - DONE for Fa17
5. en_windows_7_enterprise_with_sp1_x64_dvd_u_677651 - DONE for Fa17
6. Lolli Android-x86 5.1 RC1 - DONE for Fa17

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.

Rich's To Do List

1. pfSense (2.3.1, 64 bit) - configure IPv6
2. Kali solution for permanent DNS search string config with Network Manager

Admonition

Unauthorized hacking is a crime.

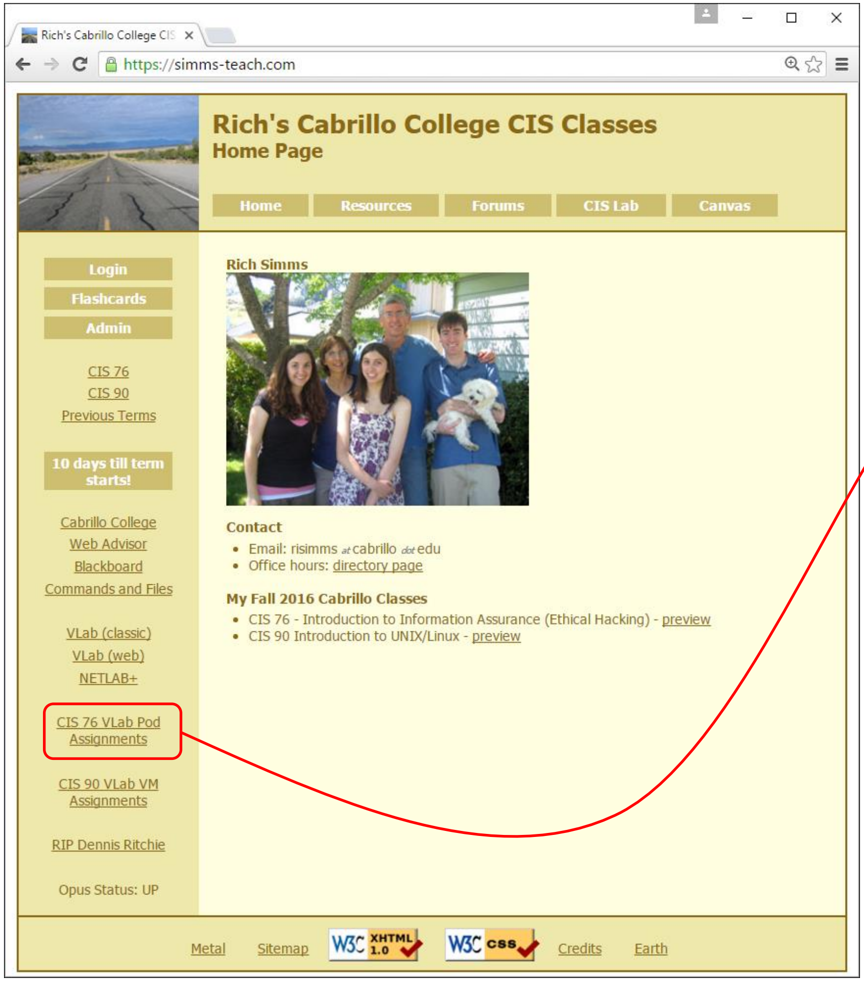
The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

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/



Rich's Cabrillo College CIS

https://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

Rich Simms

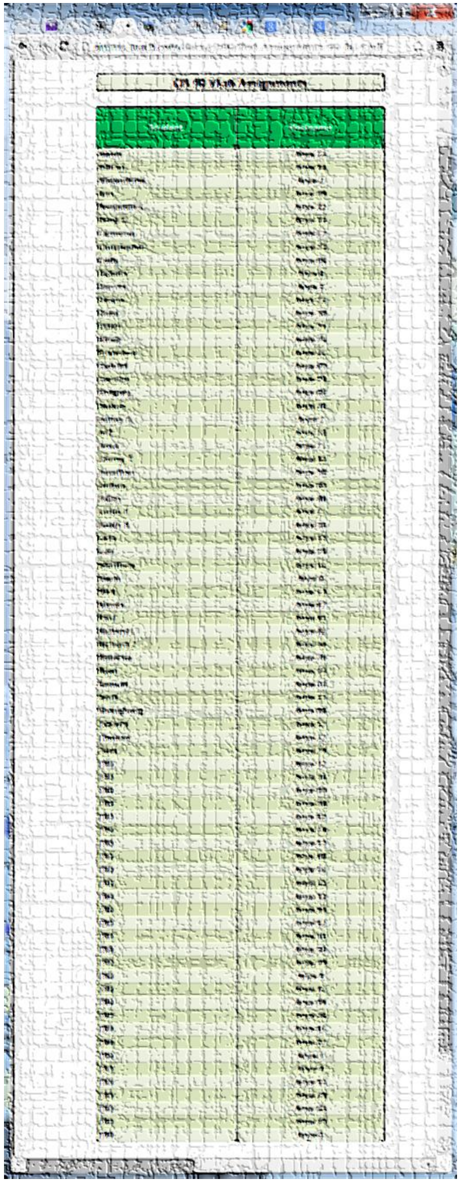
Contact

- Email: risimms at cabrillo dot edu
- Office hours: directory page

My Fall 2016 Cabrillo Classes

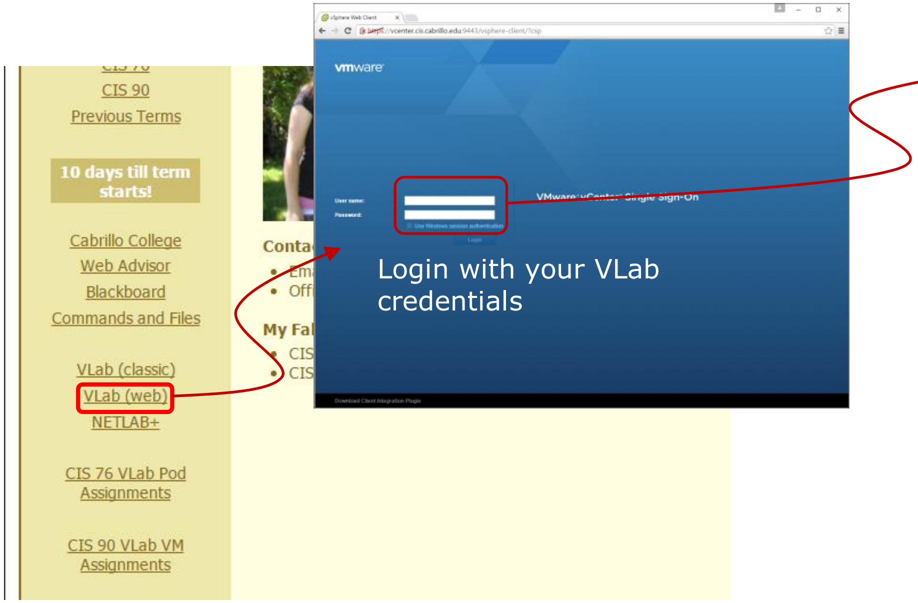
- CIS 76 - Introduction to Information Assurance (Ethical Hacking) - preview
- CIS 90 Introduction to UNIX/Linux - preview

Metal | Sitemap | W3C XHTML 1.0 | W3C CSS | Credits | Earth



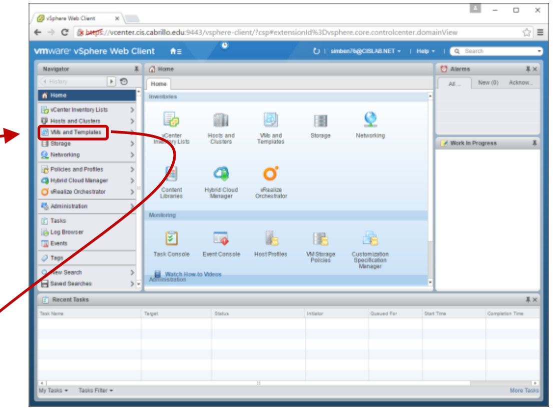
To see which pod is yours use the link on the class website

Accessing VLab
(vSphere Web Client via HTTPS)

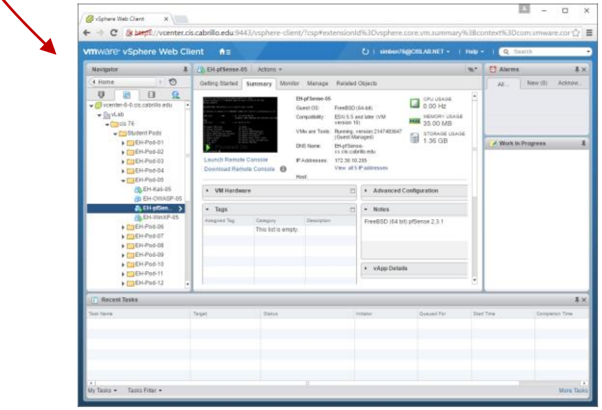

CIS 90
Previous Terms
10 days till term starts!
Cabrillo College
Web Advisor
Blackboard
Commands and Files
VLab (classic)
VLab (web)
NETLAB+
CIS 76 VLab Pod Assignments
CIS 90 VLab VM Assignments
vmware
VMware vCenter Single Sign-On
User name:
Password:
Use Windows session authentication
Login

Login with your VLab credentials

http://simms-teach.com/



Select VM and Templates

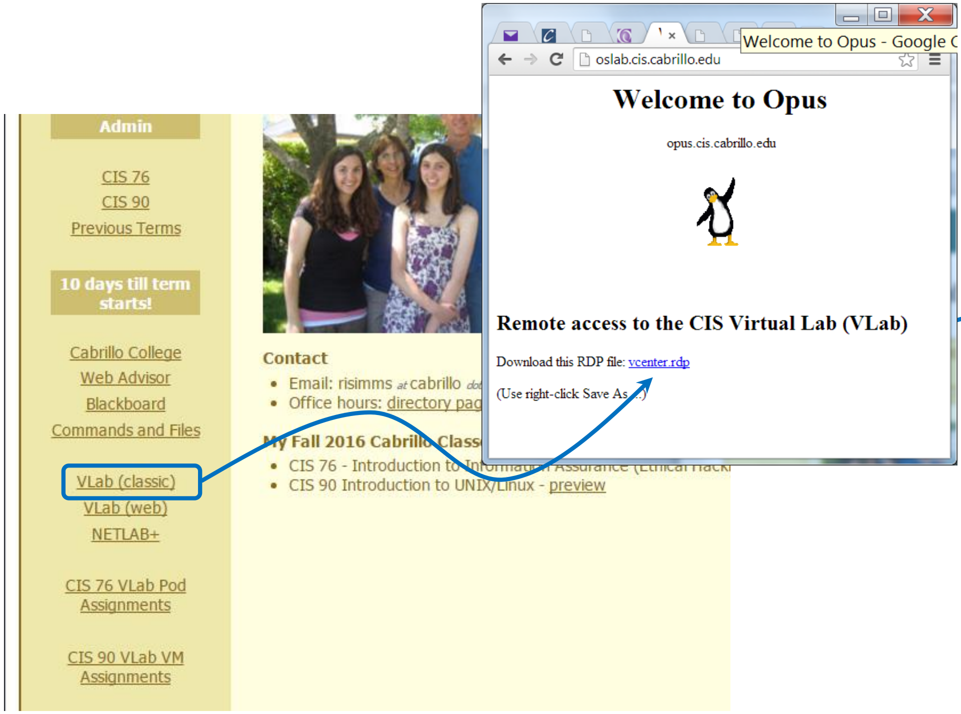


Expand containers and locate your pod VMs

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*)



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 at cabrillo do
- Office hours: directory pag

My Fall 2016 Cabrillo Class

- CIS 76 - Introduction to Information Assurance (Ethical Hack
- CIS 90 Introduction to UNIX/Linux - preview

Welcome to Opus - Google C

oslab.cis.cabrillo.edu

Welcome to Opus

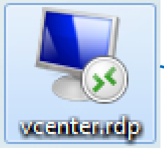
opus.cis.cabrillo.edu

Remote access to the CIS Virtual Lab (VLab)

Download this RDP file: vcenter.rdp

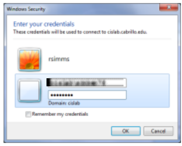
(Use right-click Save As ...)

1



vcenter.rdp

Open



Windows Security

Enter your credentials

These credentials will be used to connect to cislab.cabrillo.edu.

rsimms

[redacted]

••••••••

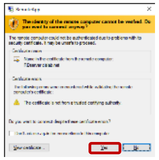
Domain: cislab

□ Remember my credentials

OK Cancel

Login with VLab credentials

2



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
TSserver.cislab.net

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

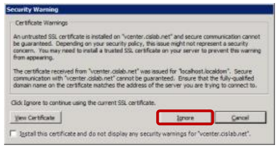
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

View certificate... Yes No

Yes, Connect



Security Warning

Certificate Warnings

An untrusted SSL certificate is installed on "vcenter.cislab.net" and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern. You may need to install a trusted SSL certificate on your server to prevent this warning from appearing.

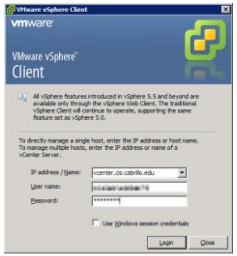
The certificate received from "vcenter.cislab.net" was issued for "localhost.localdom". Secure communication with "vcenter.cislab.net" cannot be guaranteed. Ensure that the fully-qualified domain name on the certificate matches the address of the server you are trying to connect to.

Click Ignore to continue using the current SSL certificate.

View Certificate Ignore Cancel

□ Install this certificate and do not display any security warnings for "vcenter.cislab.net".

Ignore



VMware vSphere Client

vmware

VMware vSphere Client

All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: vcenter.cis.cabrillo.edu

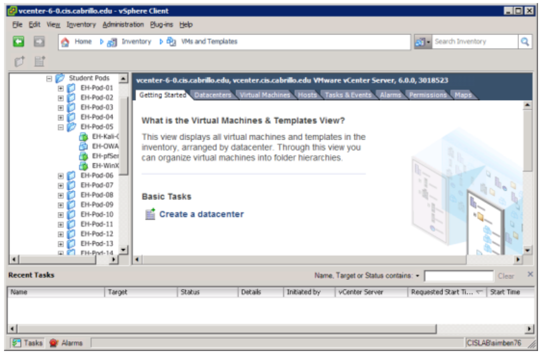
User name: [redacted]

Password: ********

□ Use Windows session credentials

Login Close

Wait ... **



vcenter-6-0.cis.cabrillo.edu - vSphere Client

File Edit View Inventory Administration Plug-ins Help
Home Inventory VMs and Templates
Search Inventory
Student Pods
EH-Pod-01
EH-Pod-02
EH-Pod-03
EH-Pod-04
EH-Pod-05
EH-Kali-(
EH-OWA
EH-pfSer
EH-WinX
EH-Pod-06
EH-Pod-07
EH-Pod-08
EH-Pod-09
EH-Pod-10
EH-Pod-11
EH-Pod-12
EH-Pod-13
EH-Pod-14
Getting Started Datacenters Virtual Machines Hosts Tasks & Events Alarms Permissions Maps
Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by vCenter Server Requested Start Ti... Start Time
Tasks Alarms

vcenter-6-0.cis.cabrillo.edu, vcenter.cis.cabrillo.edu VMware vCenter Server, 6.0.0, 3018523

What is the Virtual Machines & Templates View?

This view displays all virtual machines and templates in the inventory, arranged by datacenter. Through this view you can organize virtual machines into folder hierarchies.

Basic Tasks

Create a datacenter

CISLAB\simben76

VMs and Templates view

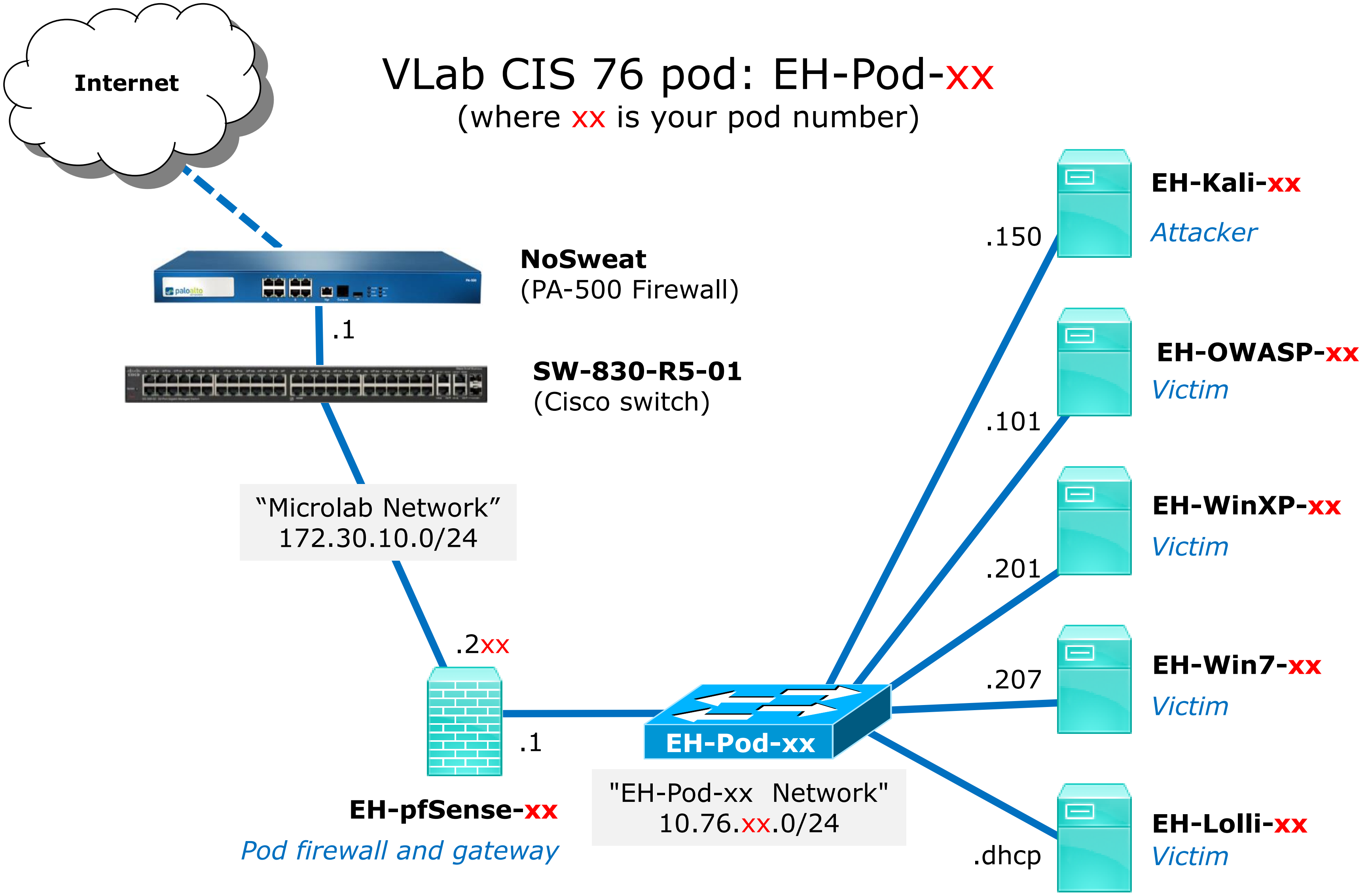
*Mac users will need to install an RDP like the Microsoft Remote Desktop app.

**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".

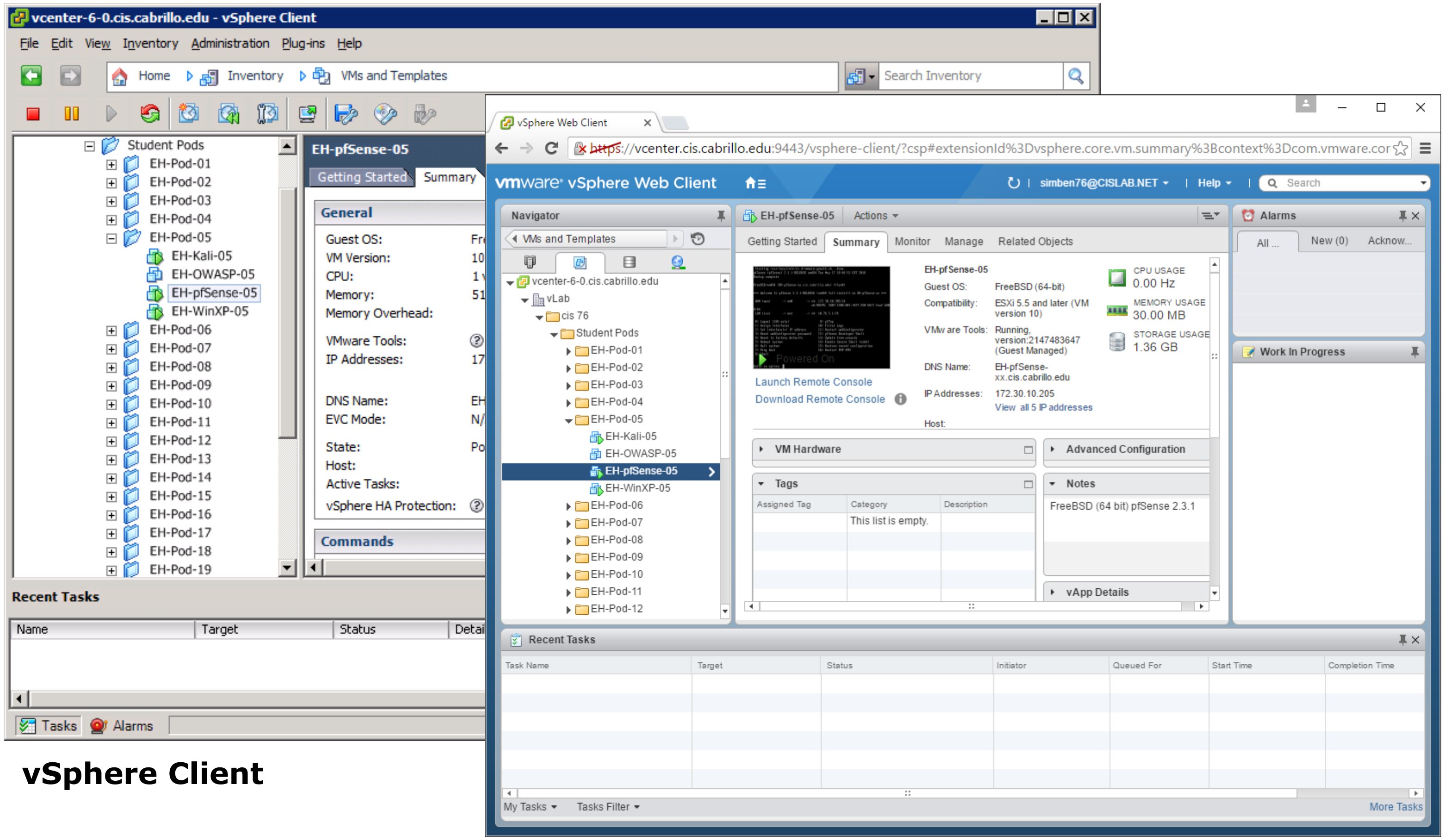
CIS 76 - VLab Pod Setup

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



CIS VLab (Virtual Lab) Student Pods



vSphere Client – EH-pfSense-05, Summary, General:

Guest OS: Fr
VM Version: 10
CPU: 1 v
Memory: 51
Memory Overhead:
VMware Tools:
IP Addresses: 17
DNS Name: EH
EVC Mode: N/
State: Po
Host:
Active Tasks:
vSphere HA Protection:

Name	Target	Status	Detai

vSphere Web Client – https://vcenter.cis.cabrillo.edu:9443/vsphere-client/?csp#extensionId%3Dvsphere.core.vm.summary%3Bcontext%3Dcom.vmware.cor

EH-pfSense-05
Guest OS: FreeBSD (64-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: EH-pfSense-xx.cis.cabrillo.edu
IP Addresses: 172.30.10.205
View all 5 IP addresses
Host:

CPU USAGE 0.00 Hz
MEMORY USAGE 30.00 MB
STORAGE USAGE 1.36 GB

Assigned Tag	Category	Description
	This list is empty.	

Notes: FreeBSD (64 bit) pfSense 2.3.1

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time

vSphere Client

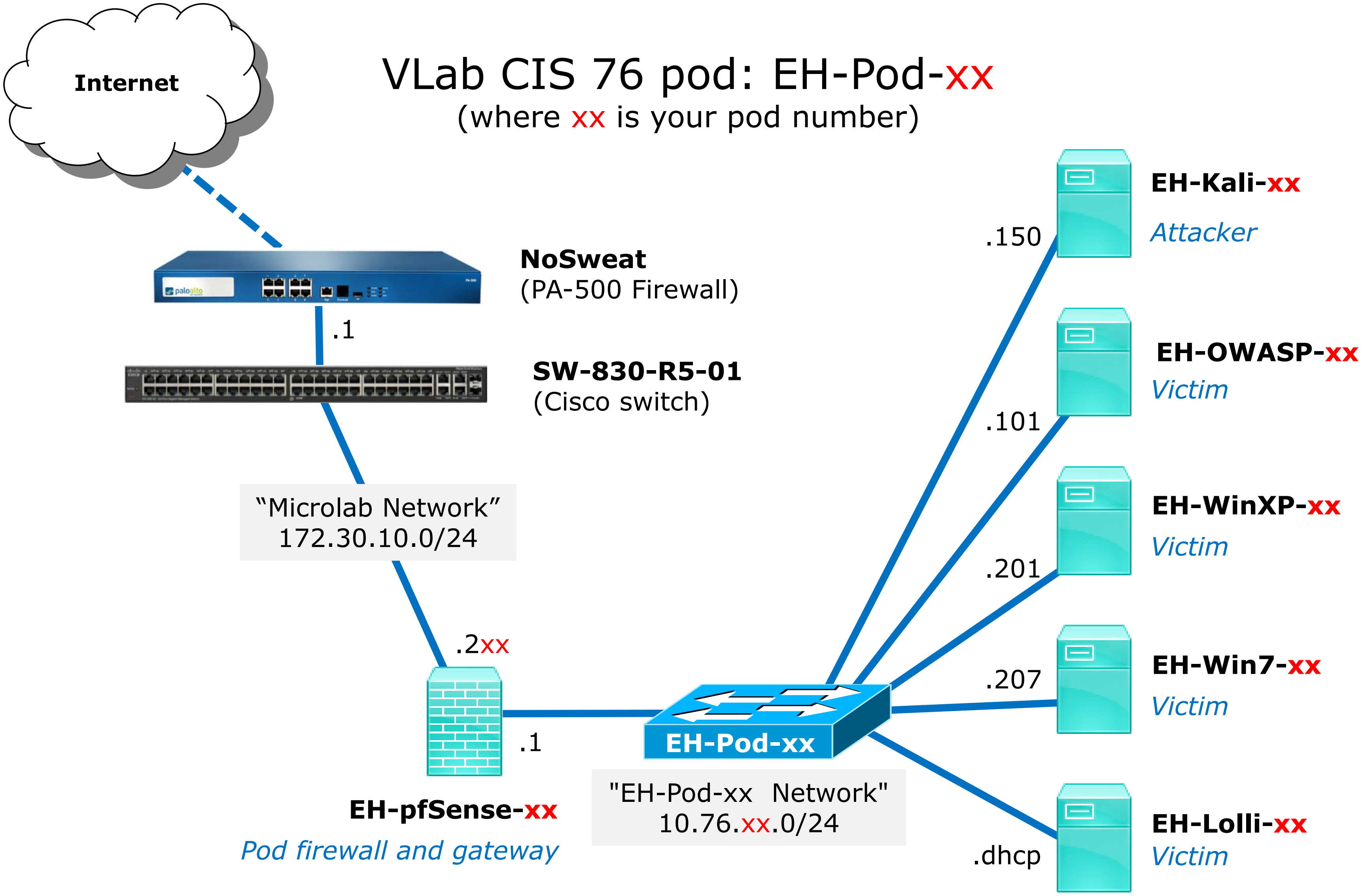
vSphere Web Client

Students can use either vSphere Client or vSphere Web Client

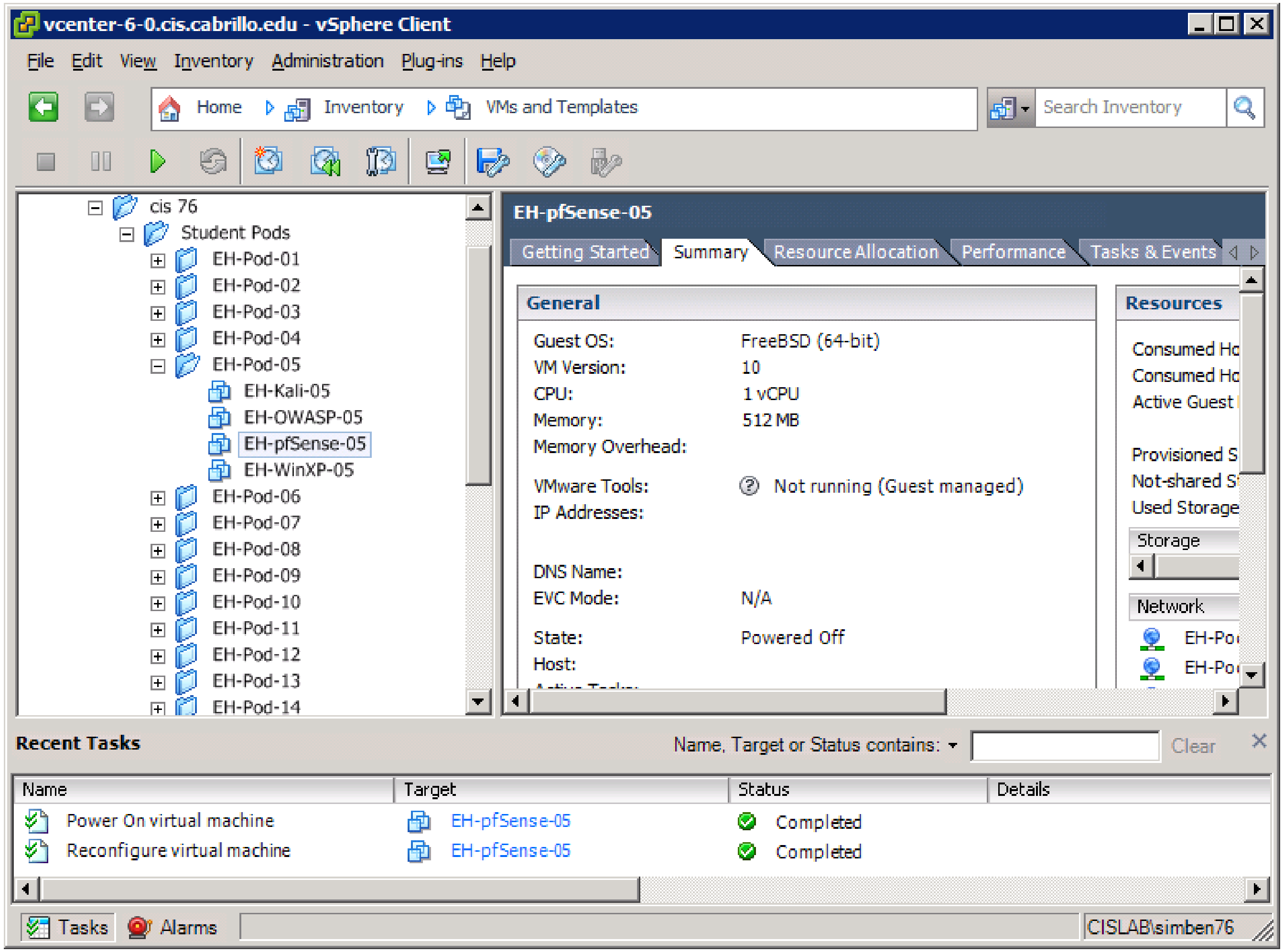
EH-pfSense-xx VM Config

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



CIS VLab (Virtual Lab) Student Pods



vcenter-6-0.cis.cabrillo.edu - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory VMs and Templates
Search Inventory
Getting Started Summary Resource Allocation Performance Tasks & Events
Resources
Consumed Ho
Consumed Ho
Active Guest
Provisioned S
Not-shared S
Used Storage
Storage
Network
EH-Po
EH-Po
Clear
Tasks Alarms
CISLAB\simben76

- 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
    - EH-Pod-08
    - EH-Pod-09
    - EH-Pod-10
    - EH-Pod-11
    - EH-Pod-12
    - EH-Pod-13
    - EH-Pod-14

EH-pfSense-05

General

Guest OS:	FreeBSD (64-bit)
VM Version:	10
CPU:	1 vCPU
Memory:	512 MB
Memory Overhead:	
VMware Tools:	Not running (Guest managed)
IP Addresses:	
DNS Name:	
EVC Mode:	N/A
State:	Powered Off
Host:	

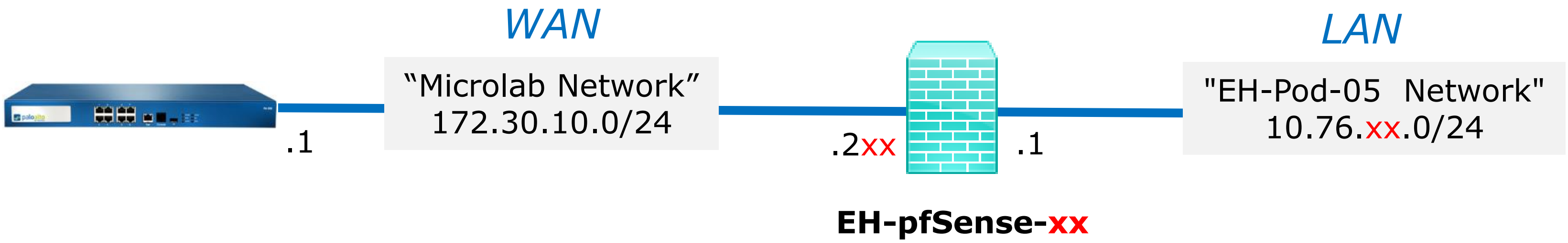
Recent Tasks

Name, Target or Status contains:

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.

Configuring the EH-pfSense VM in EH-Pod-xx



WAN

“Microlab Network”
172.30.10.0/24

LAN

"EH-Pod-05 Network"
10.76.xx.0/24

.1

.2xx

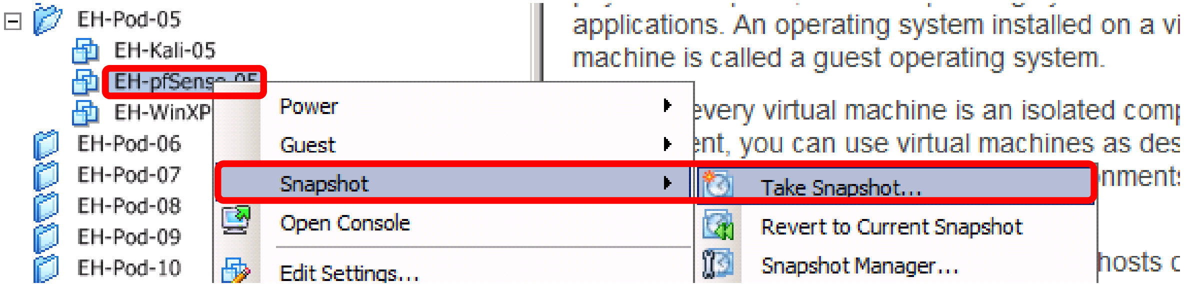
.1

EH-pfSense-xx

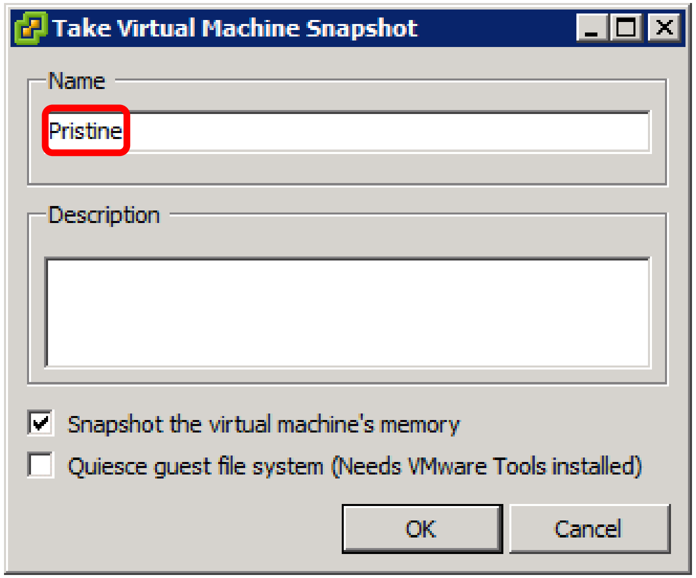
pfSense VM	Pod xx settings
VM Network Adapter 1	uLab Net
VM Network Adapter 2	EH-Pod-xx Net
Hostname	EH-pfSense-xx
WAN IPv4	172.30.10.2xx
WAN subnet bits	24
WAN upstream gateway	172.30.10.1
WAN IPv6	DHCP6
LAN webConfigurator	Use HTTPS
LAN IPv4	10.76.x.1
LAN subnet bits	24
LAN DHCP service	10.76.x.50 - 10.76.x.99
LAN webConfigurator	Use HTTPS

xx is the pod number assigned to you.

Configuring the EH-pfSense VM in EH-Pod-xx


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
Power
Guest
Snapshot
Open Console
Edit Settings...
Take Snapshot...
Revert to Current Snapshot
Snapshot Manager...
applications. An operating system installed on a vi
machine is called a guest operating system.
every virtual machine is an isolated comp
ent, you can use virtual machines as des
nments
hosts c

Pod 5 example



Name: Pristine

Description:

☑ Snapshot the virtual machine's memory

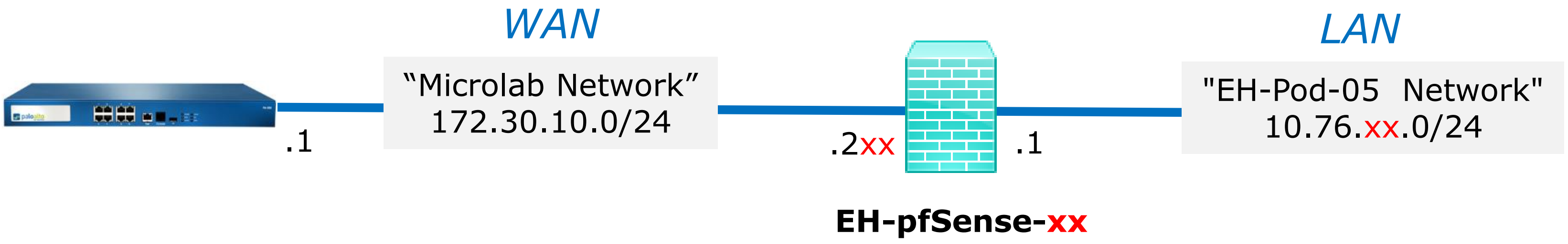
□ Quiesce guest file system (Needs VMware Tools installed)

IMPORTANT, back up your VM!

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

Now if you mess things up you can always start over again!

Configuring the EH-pfSense VM in EH-Pod-xx



WAN

“Microlab Network”
172.30.10.0/24

.1

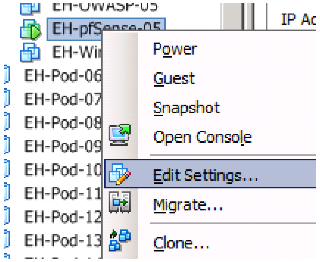
.2xx

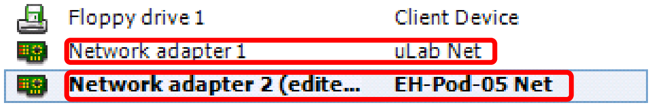
.1

LAN

"EH-Pod-05 Network"
10.76.xx.0/24

EH-pfSense-xx



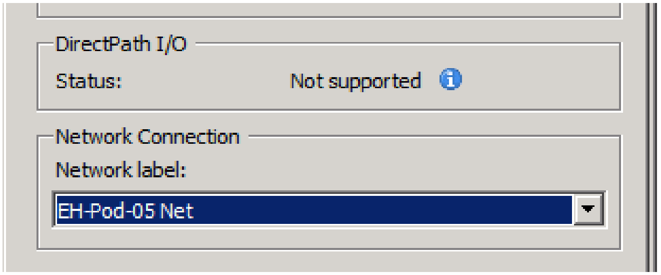


Floppy drive 1 — Client Device

Network adapter 1 — uLab Net

Network adapter 2 (edite... — EH-Pod-05 Net

Pod 5 example



DirectPath I/O

Status: Not supported

Network Connection

Network label: EH-Pod-05 Net

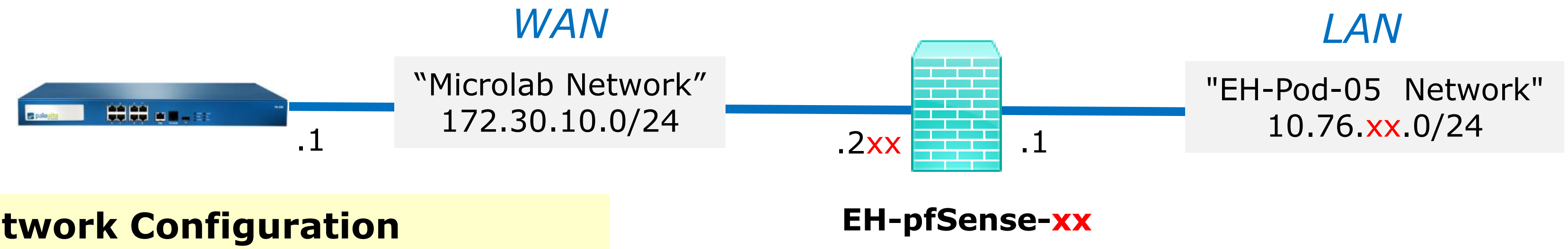
Network Cabling

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.

Configuring the EH-pfSense VM in EH-Pod-xx



Network Configuration

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

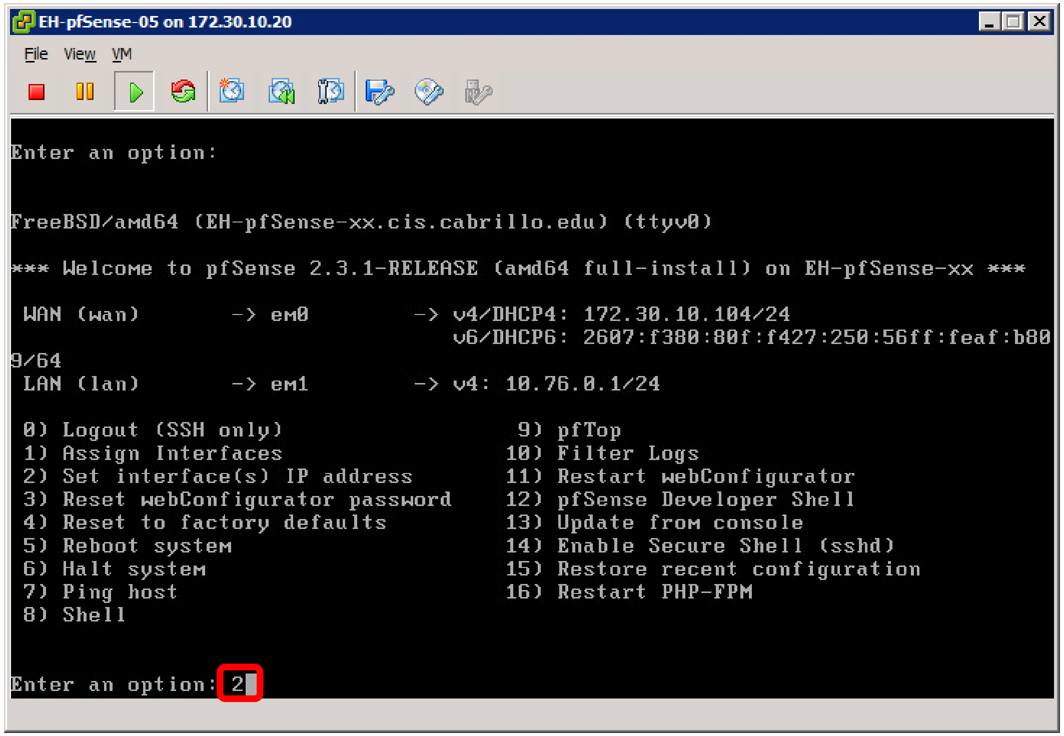
WAN: 172.30.10.2xx, where xx is your two digit pod number.

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

2) Power up the VM and open a console.

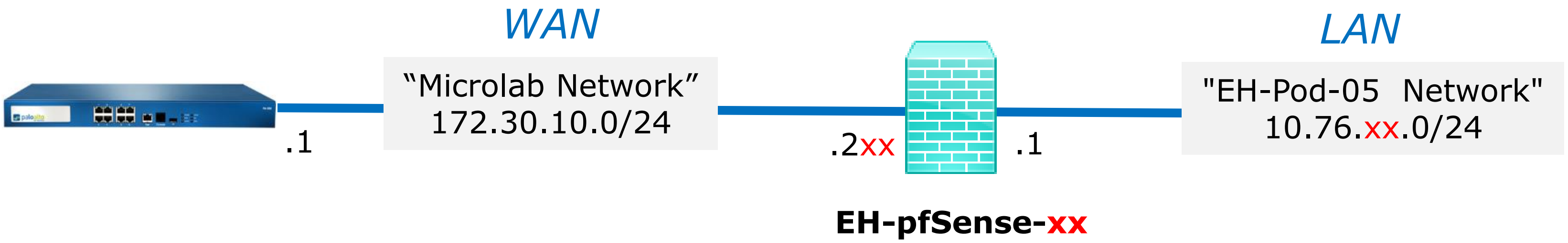
3) Wait till you see the menu options (0-16).

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



```
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
```

Configuring the EH-pfSense VM in EH-Pod-xx



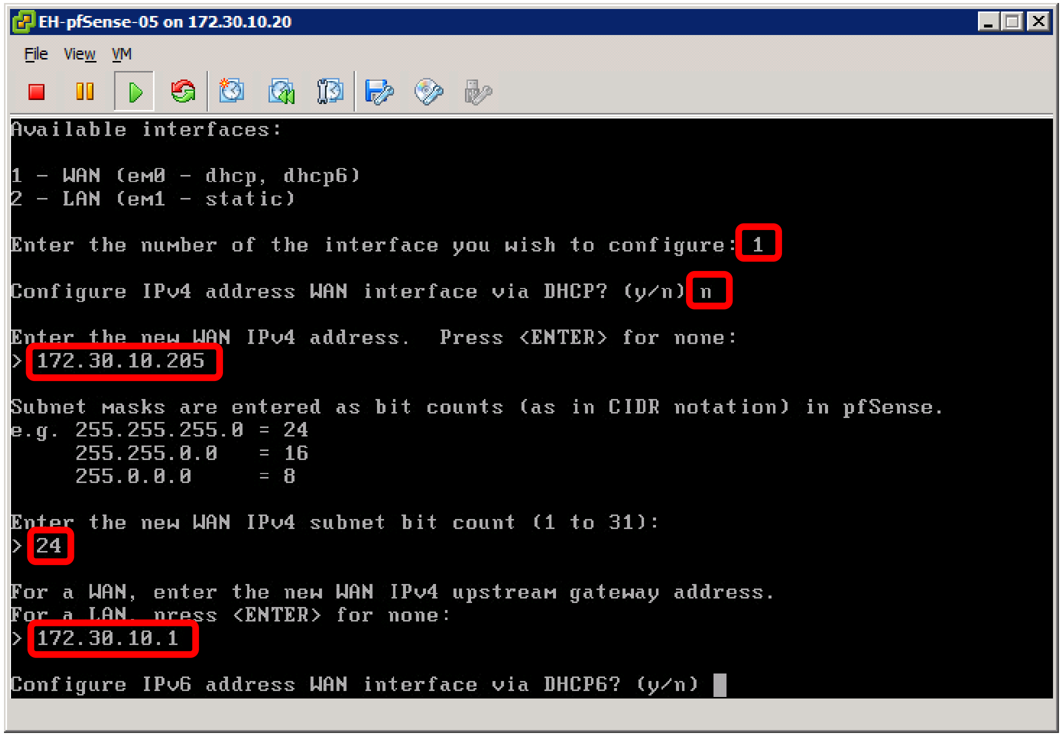
5) Select Option **1** to configure the WAN interface.

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

7) Set your outside WAN IP address to **172.30.10.2xx** where xx is your two digit pod number. For example, Pod 5's WAN IP address will be: 172.30.10.205

8) Select **24** bits for the subnet mask.

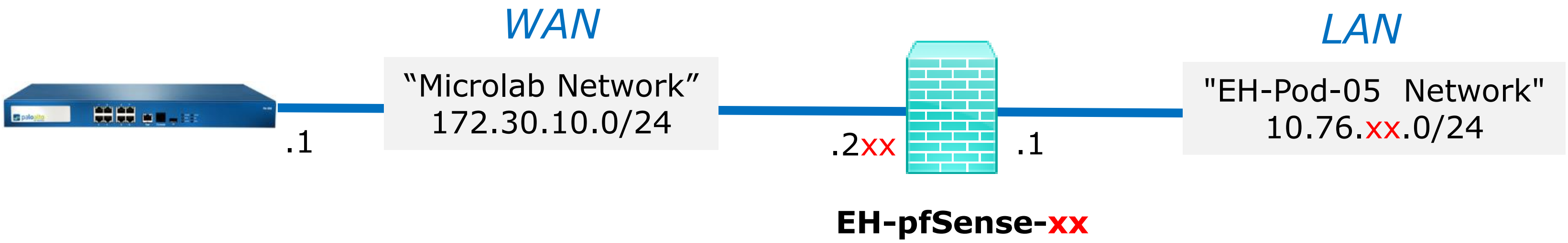
9) Set the upstream gateway to: **172.30.10.1**

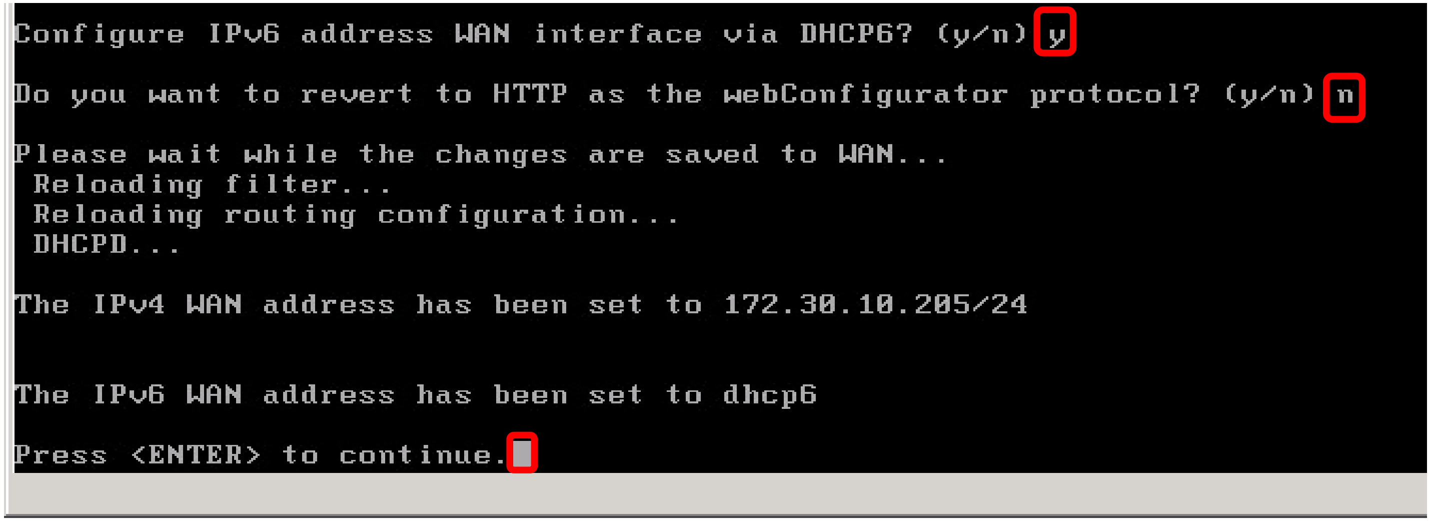


```
Available interfaces:

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)
```

Pod 5 example

Configuring the EH-pfSense VM in EH-Pod-xx





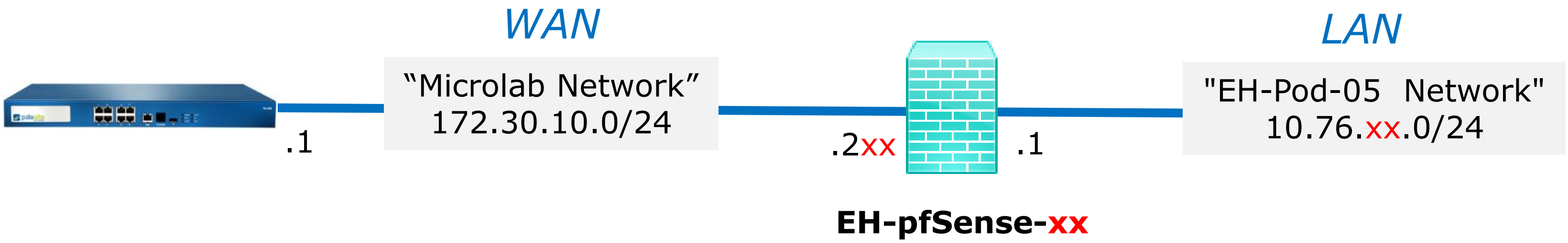
```
Configure IPv6 address WAN interface via DHCP6? (y/n) y

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.
```

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

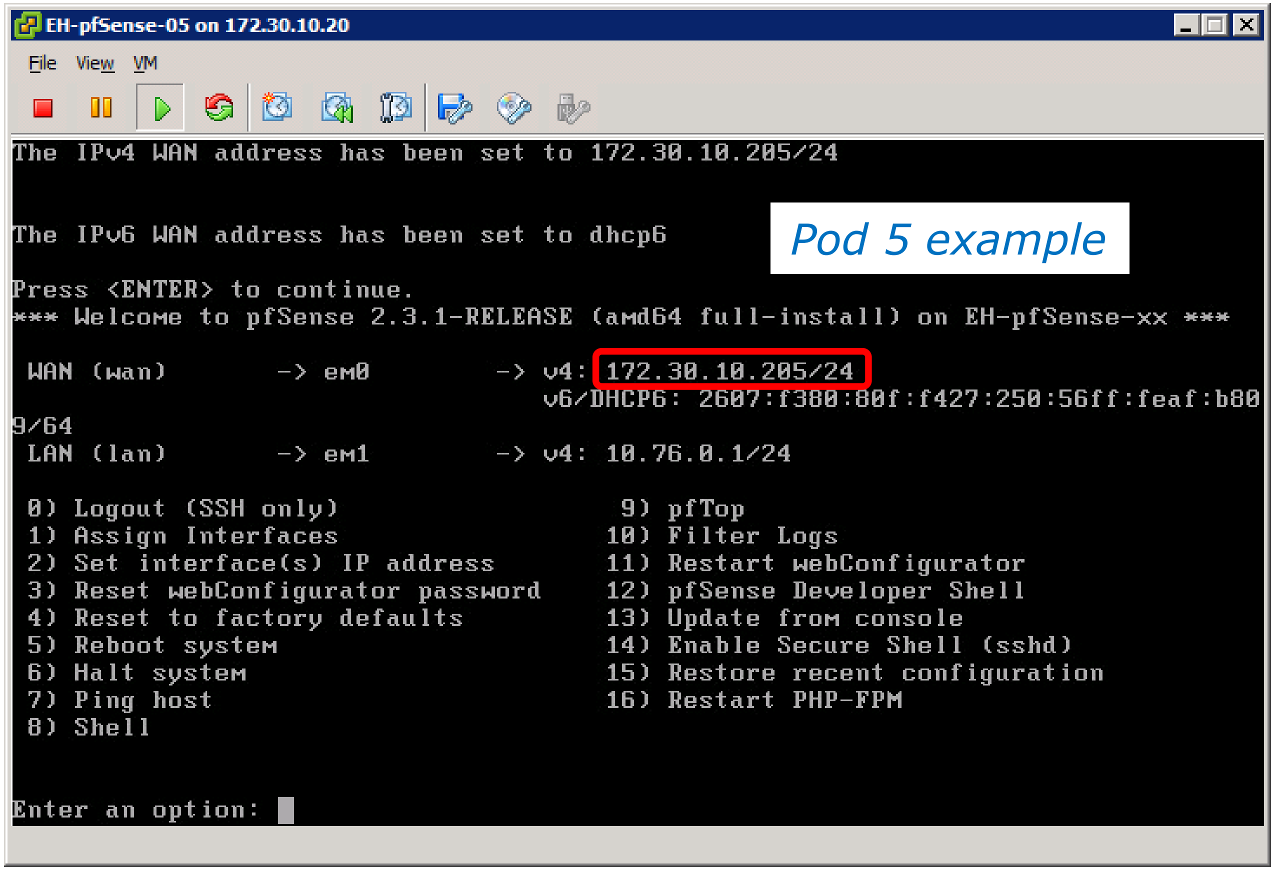
11) Enter "**n**" to not revert to HTTP as the webConfigurator protocol.

12) Press **<ENTER>** to continue.

Configuring the EH-pfSense VM in EH-Pod-xx



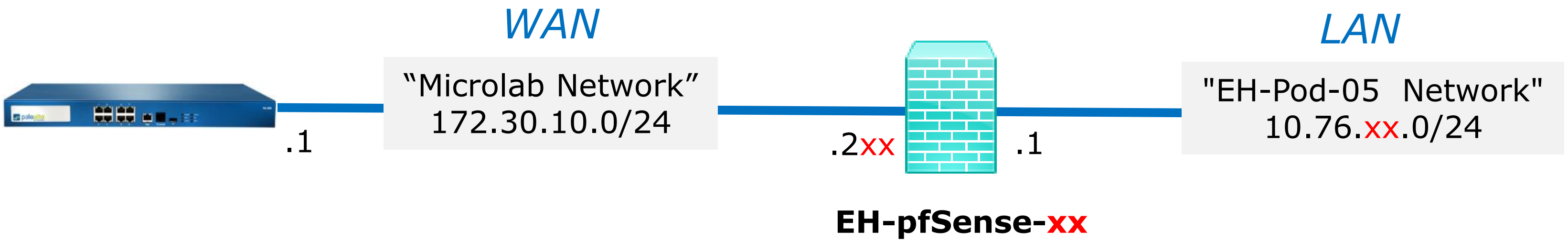
13) Verify the WAN interface IP address is **172.30.10.2xx/24** where xx is your pod number.



Pod 5 example

```
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
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:
```

Configuring the EH-pfSense VM in EH-Pod-xx



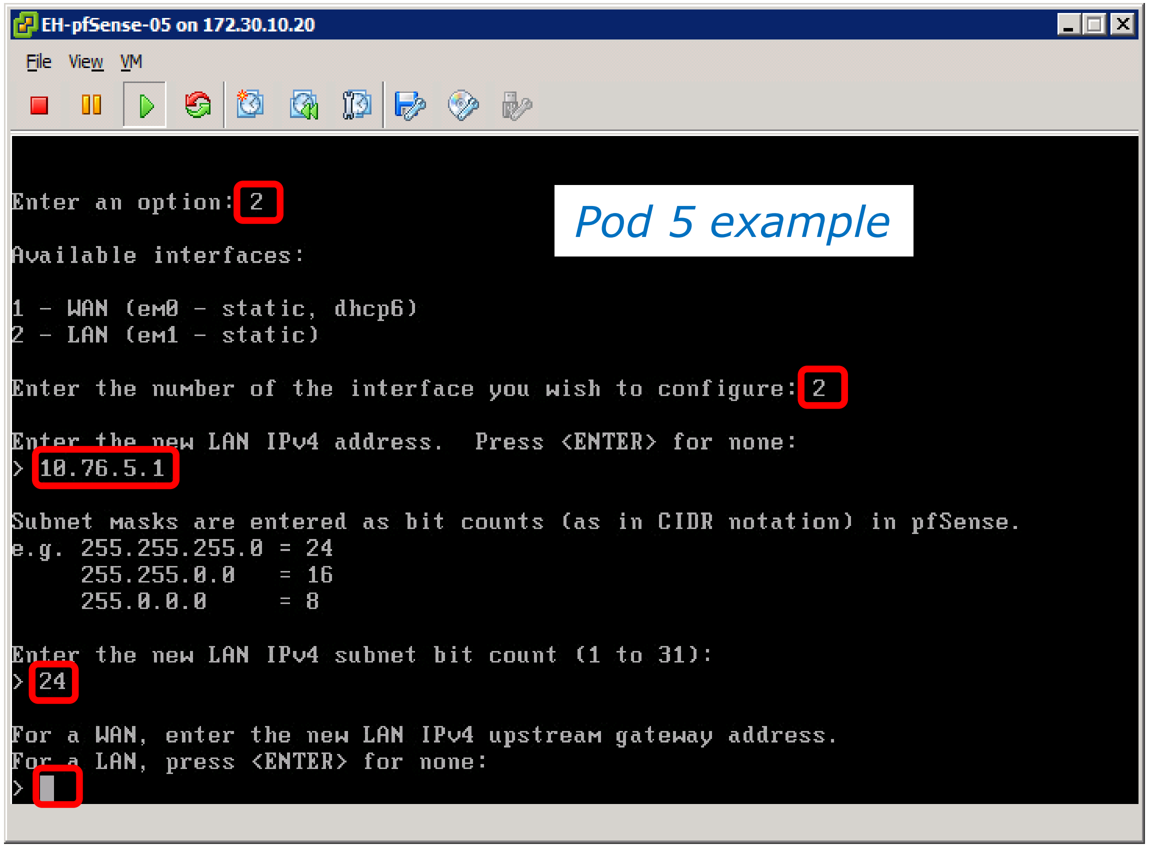
14) Select option **2** again on the main menu to set an IP address on an interface.

15) Select option **2** for LAN.

16) Set your LAN IP address to **10.76.xx.1** where xx is your pod number. For example, the Pod 5 IP address is: 10.76.5.1

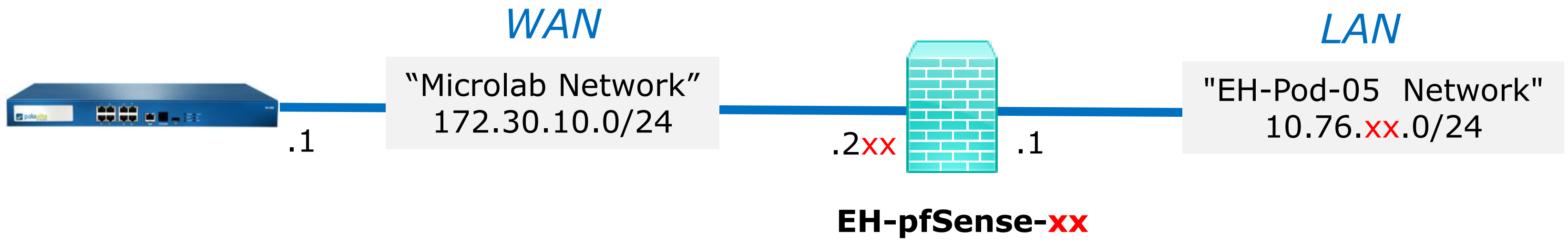
17) Select **24** bits for the subnet mask.

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



```
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:
>
```

Configuring the EH-pfSense VM in EH-Pod-xx



WAN

“Microlab Network”
172.30.10.0/24

.1

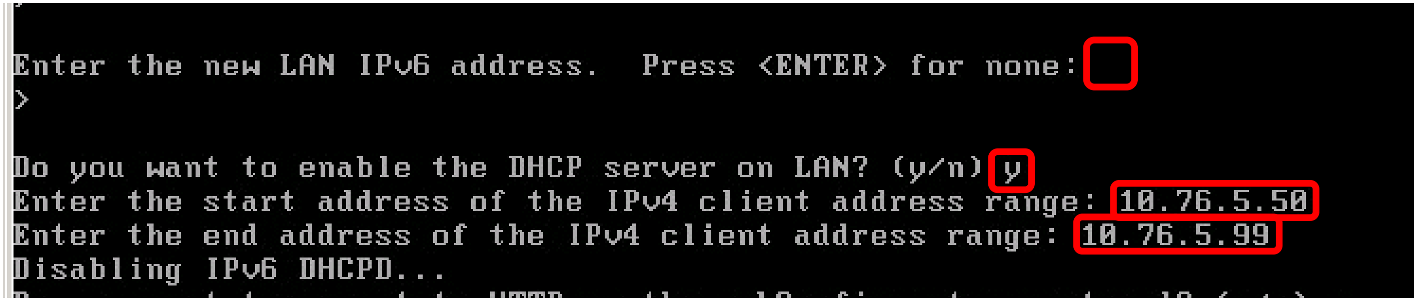
.2xx

.1

LAN

"EH-Pod-05 Network"
10.76.xx.0/24

EH-pfSense-xx



```
Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.76.5.50
Enter the end address of the IPv4 client address range: 10.76.5.99
Disabling IPv6 DHCPD...
```

Pod 5 example

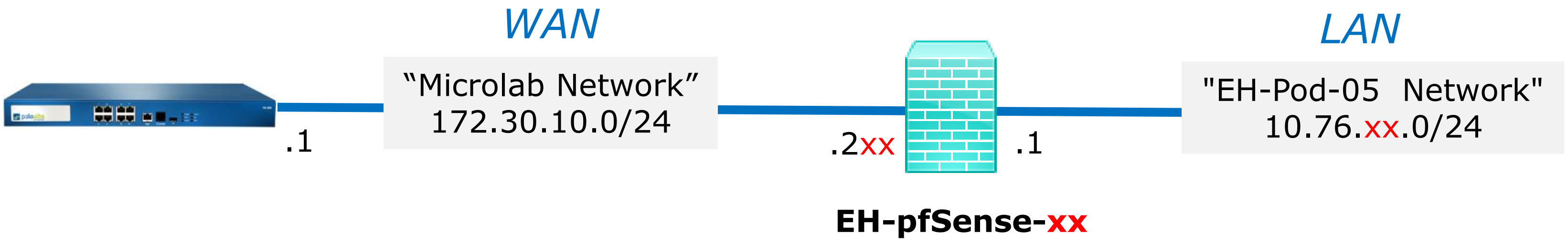
19) Press **<ENTER>** for none when prompted for the IPv6 address.

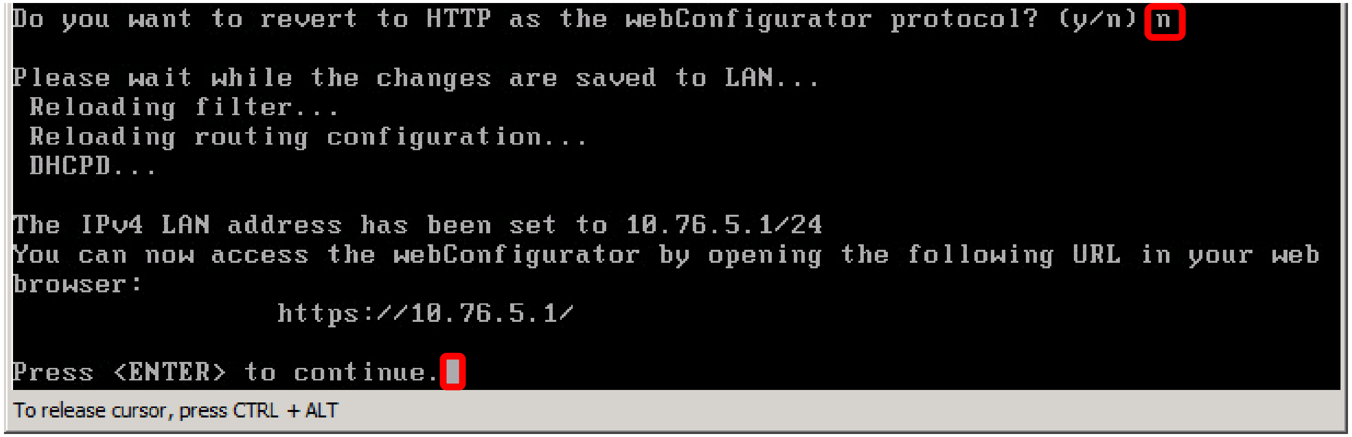
20) Enter "**y**" to setup DHCP.

21) Set the starting address to **10.76.xx.50** where xx is your pod number.

22) Set the end address to **10.76.xx.99** where xx is your pod number.

Configuring the EH-pfSense VM in EH-Pod-xx



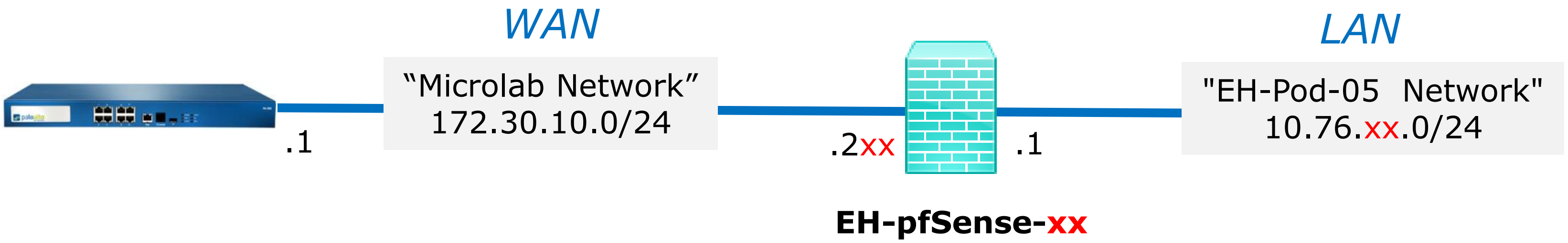


```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

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.
```

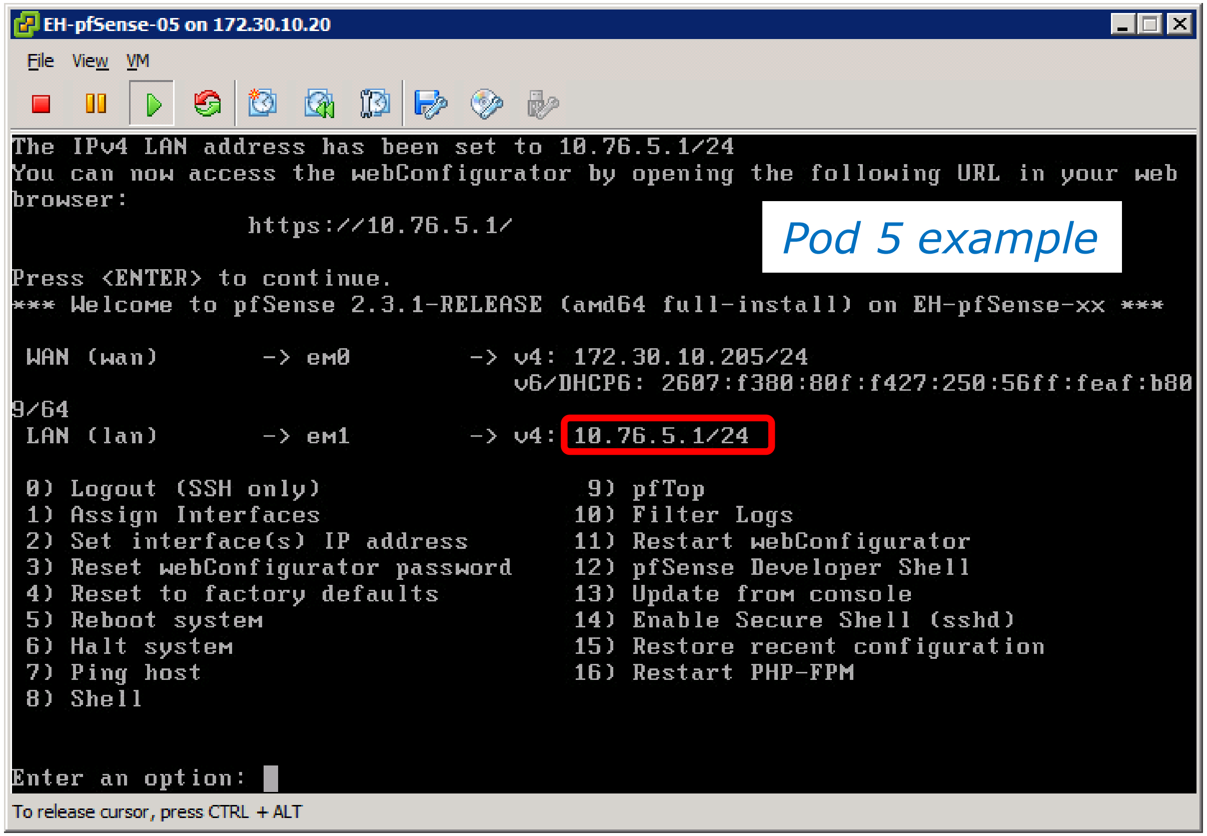
23) Enter "**n**" to not revert to HTTP for the webConfigurator. We will be using HTTPS.

24) Press **<ENTER>** to continue.

Configuring the EH-pfSense VM in EH-Pod-xx



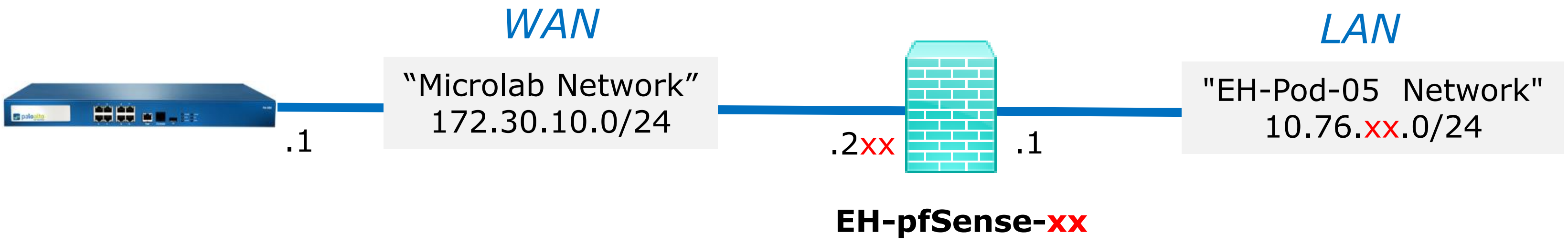
25) Verify the IP address on your LAN interface is **10.76.xx.1/24** where xx is your pod number.


EH-pfSense-05 on 172.30.10.20
File View VM
To release cursor, press CTRL + ALT

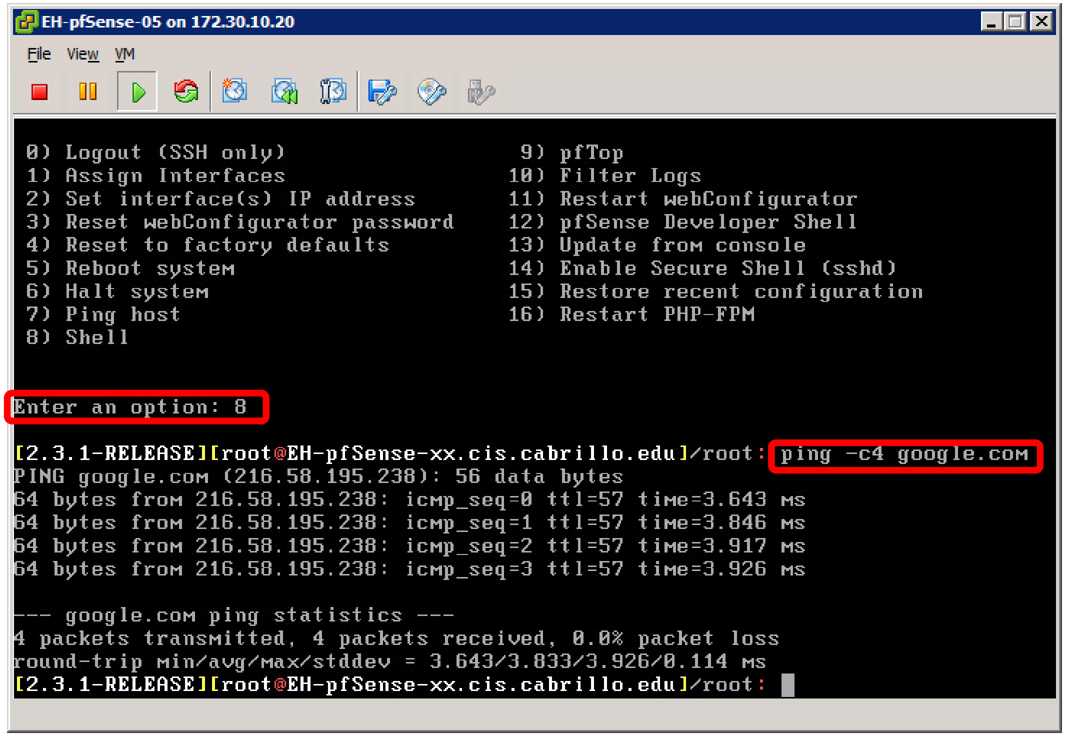
Pod 5 example

```
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:
```

Configuring the EH-pfSense VM in EH-Pod-xx

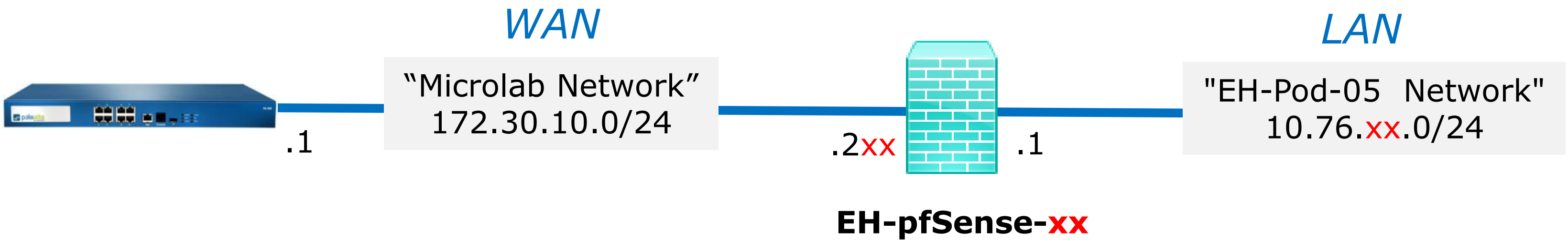


26) Select option **8** to drop into the shell and verify you have Internet connectivity by pinging google.com with:
ping -c4 google.com



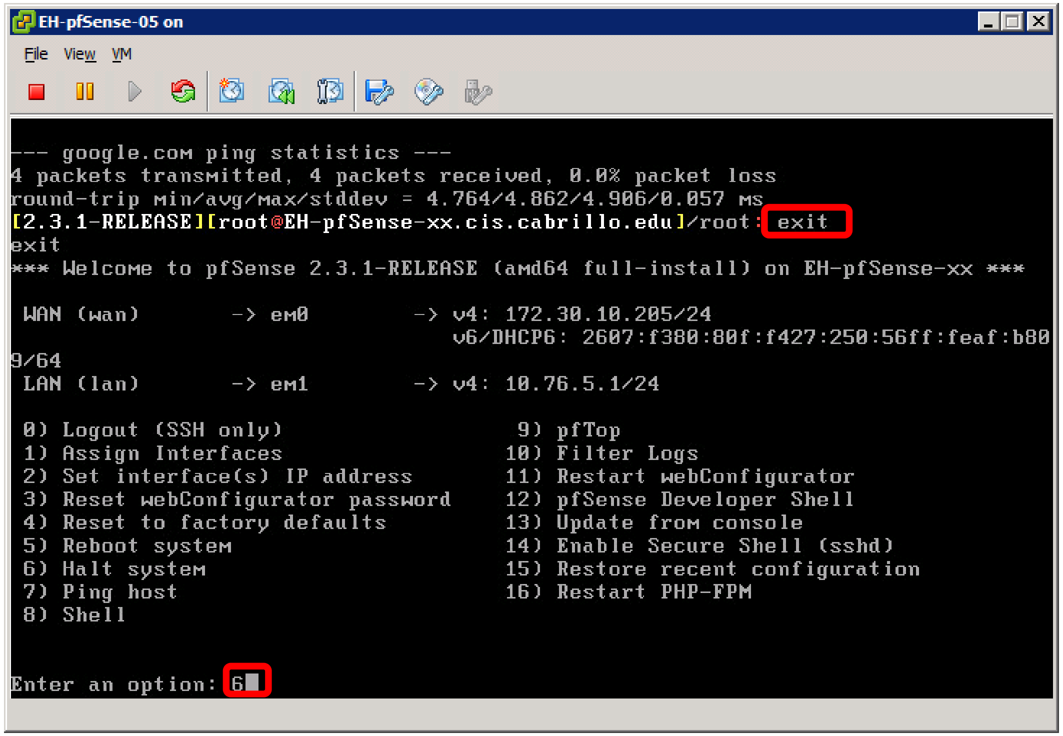
```
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Update from console
 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: 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:
```

Configuring the EH-pfSense VM in EH-Pod-xx



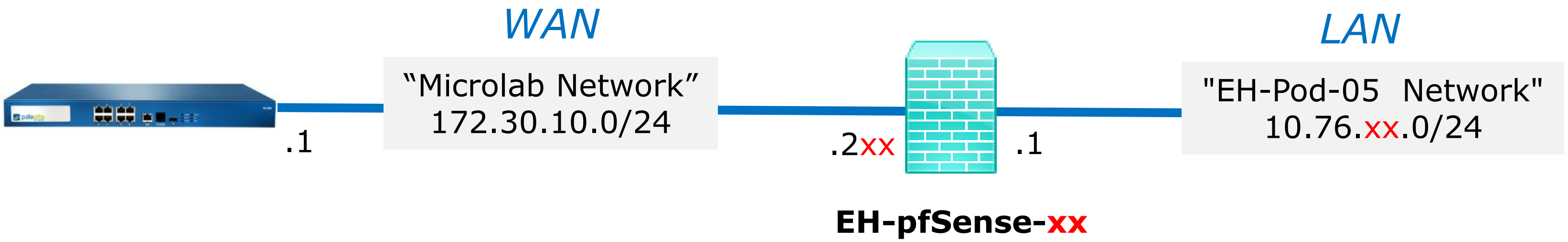
27) Type **exit** to return to the menu.

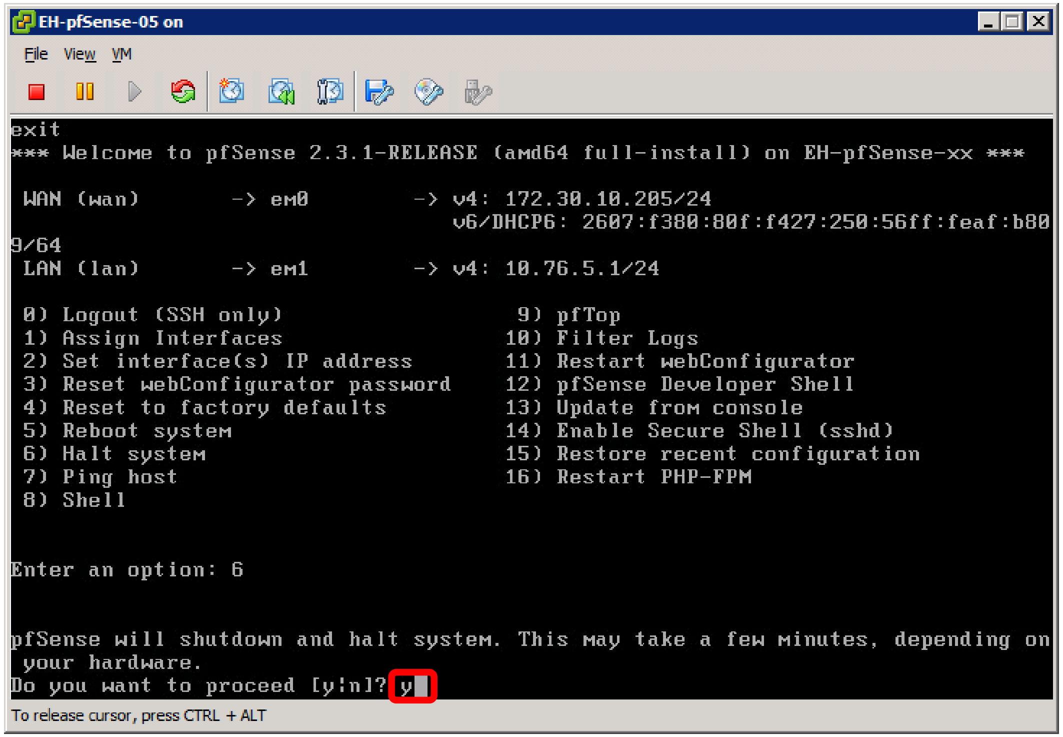
28) Select option **6** to shutdown the VM.



```
--- 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
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
```

Configuring the EH-pfSense VM in EH-Pod-xx

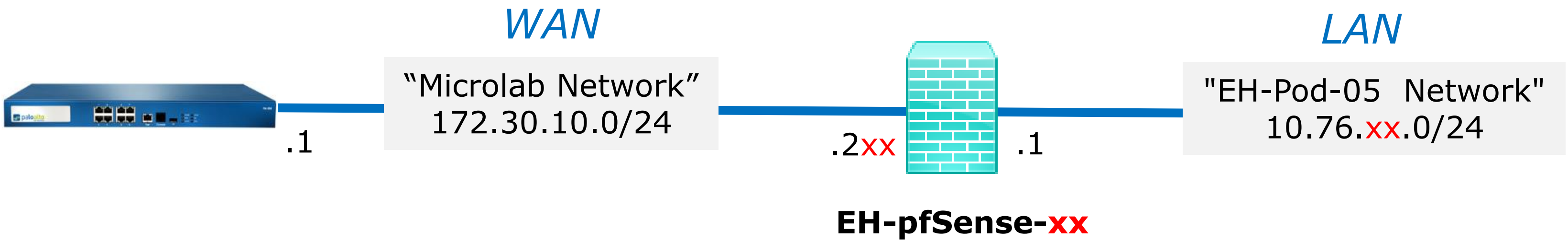




```
exit
*** Welcome to pfSense 2.3.1-RELEASE (amd64 full-install) on EH-pfSense-xx ***

 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


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

29) Type **y** to proceed.

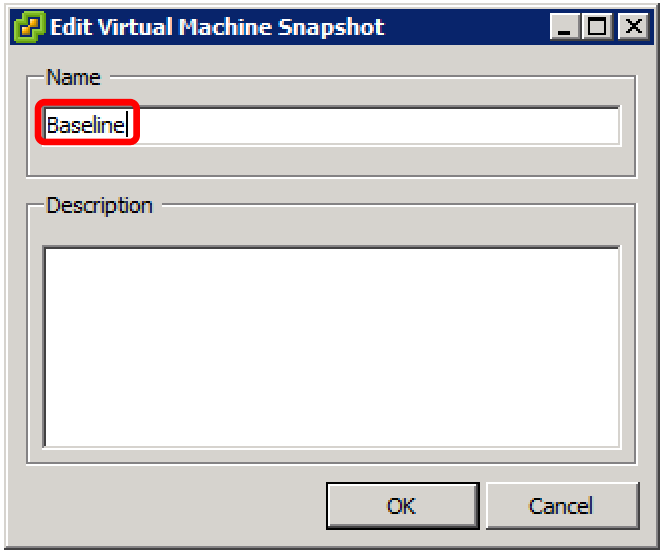
Configuring the EH-pfSense VM in EH-Pod-xx



Save your work

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

Now if you mess things up later can always start over again!


Edit Virtual Machine Snapshot

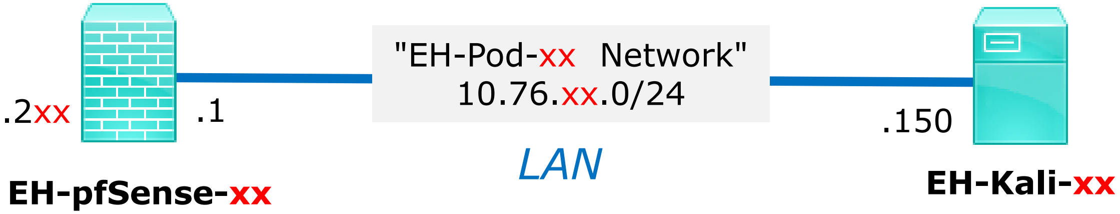
Name: Baseline

Description:

EH-pfSense-xx Port Forwarding (optional)

Configure pfSense to forward port 22 to Kali VM

Forward SSH through pfSense Firewall to Kali VM

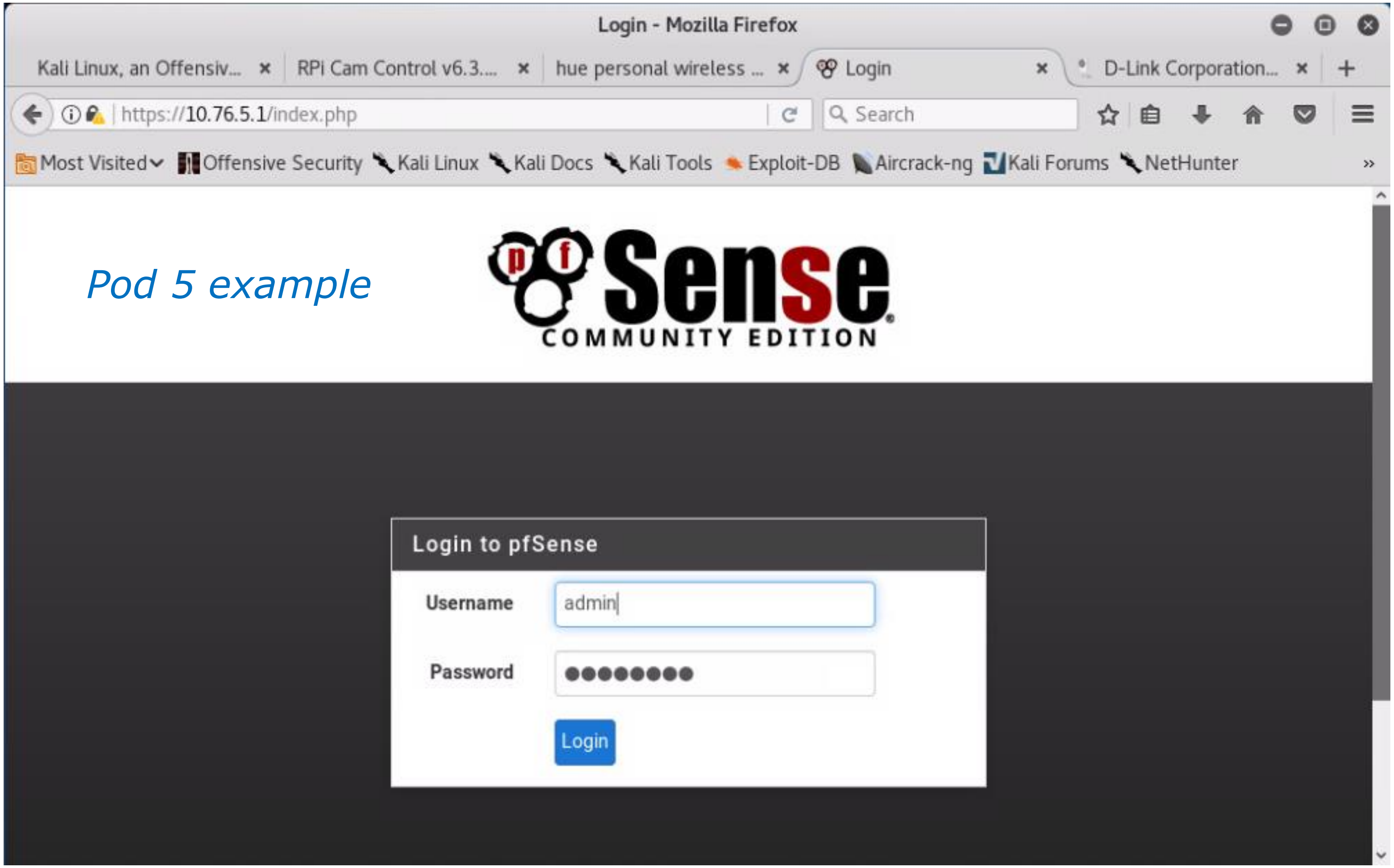


General instructions:

- From your Kali VM, browse to your pfSense VM
- Navigate to Firewall > NAT and select "Port Forward"
- Add a new rule to forward a port.
- Note, the associated filter rule is created automatically.
- From Opus-II, test that you can ssh into your Kali VM

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

Browsing from Kali to pfSense VM



Pod 5 example

https://10.76.5.1/index.php

Login to pfSense

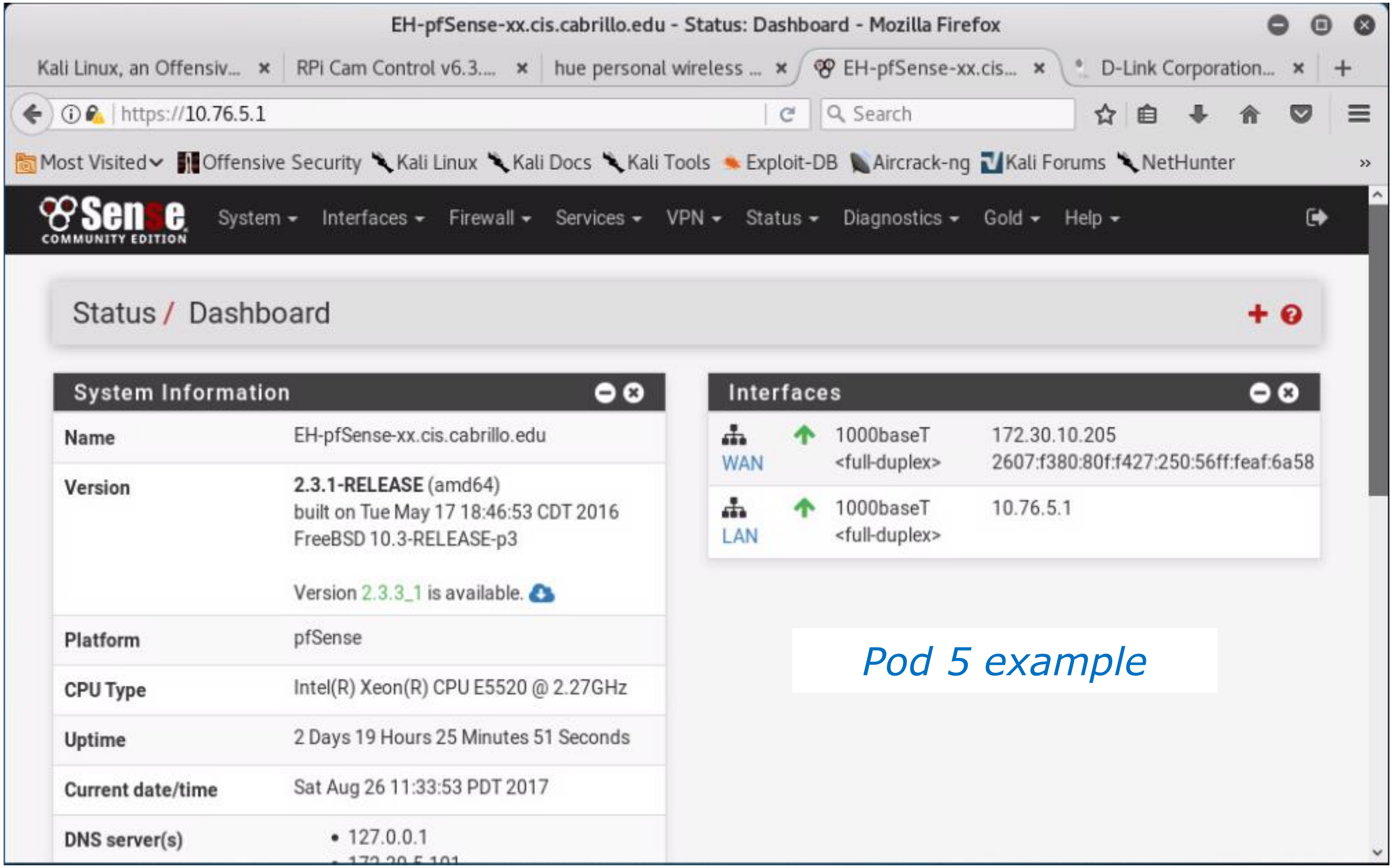
Username: admin

Password: ●●●●●●●●●

Login

On your Kali VM, browse to 10.76.xx.1, where xx is your pod number.

Browsing from Kali to pfSense VM



Status / Dashboard

System Information

Name	EH-pfSense-xx.cis.cabrillo.edu
Version	**2.3.1-RELEASE** (amd64) built on Tue May 17 18:46:53 CDT 2016 FreeBSD 10.3-RELEASE-p3 Version 2.3.3_1 is available.
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz
Uptime	2 Days 19 Hours 25 Minutes 51 Seconds
Current date/time	Sat Aug 26 11:33:53 PDT 2017
DNS server(s)	• 127.0.0.1 • 172.30.5.101

Interfaces

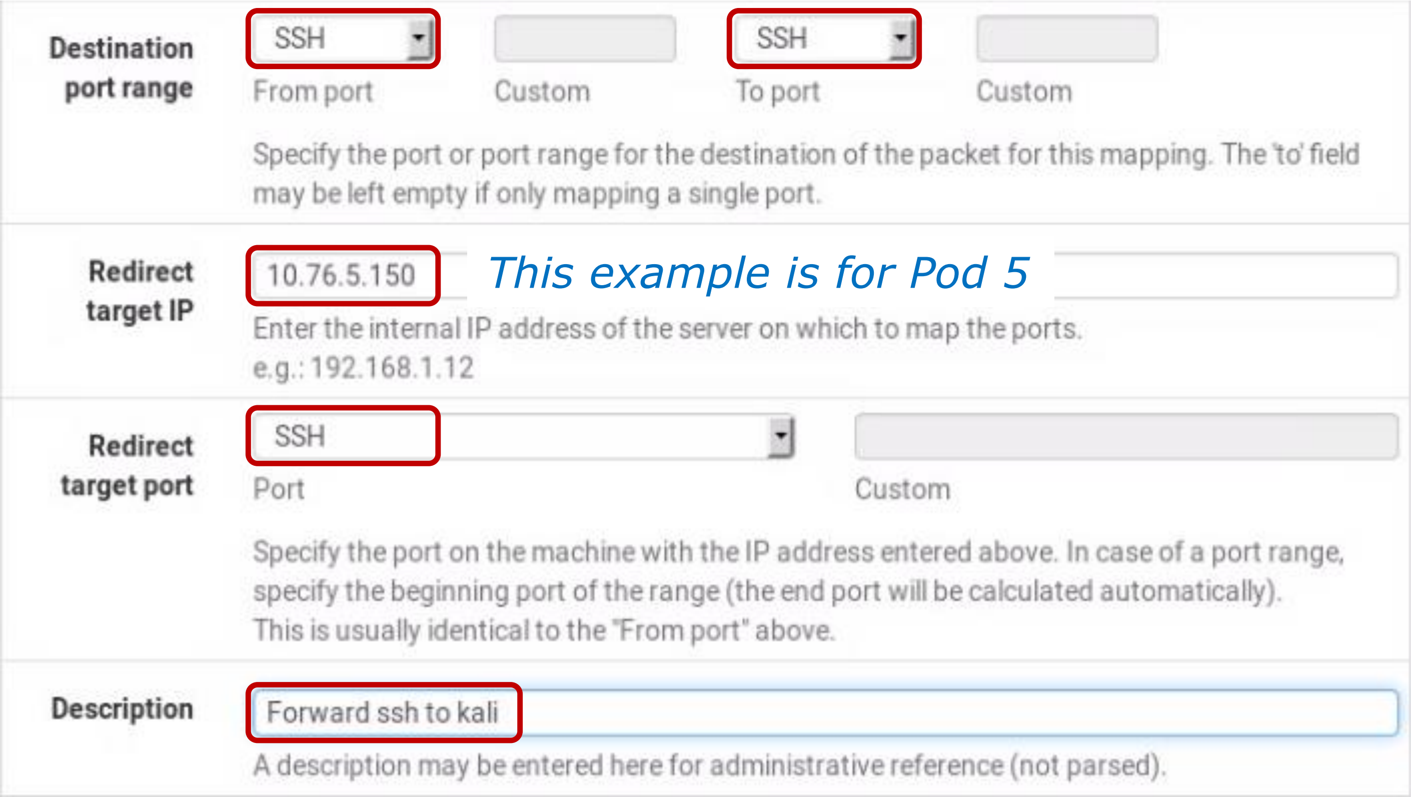
WAN	↑	1000baseT <full-duplex>	172.30.10.205 2607:f380:80f:f427:250:56ff:feaf:6a58
LAN	↑	1000baseT <full-duplex>	10.76.5.1

Pod 5 example

After logging in you can view a high level summary

Adding the new NAT Port Forward Rule

Firewall / NAT / Port Forward > "Add" button



Destination port range: SSH (From port) | Custom | SSH (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

This example is for Pod 5

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12

Redirect target port: SSH (Port) | Custom

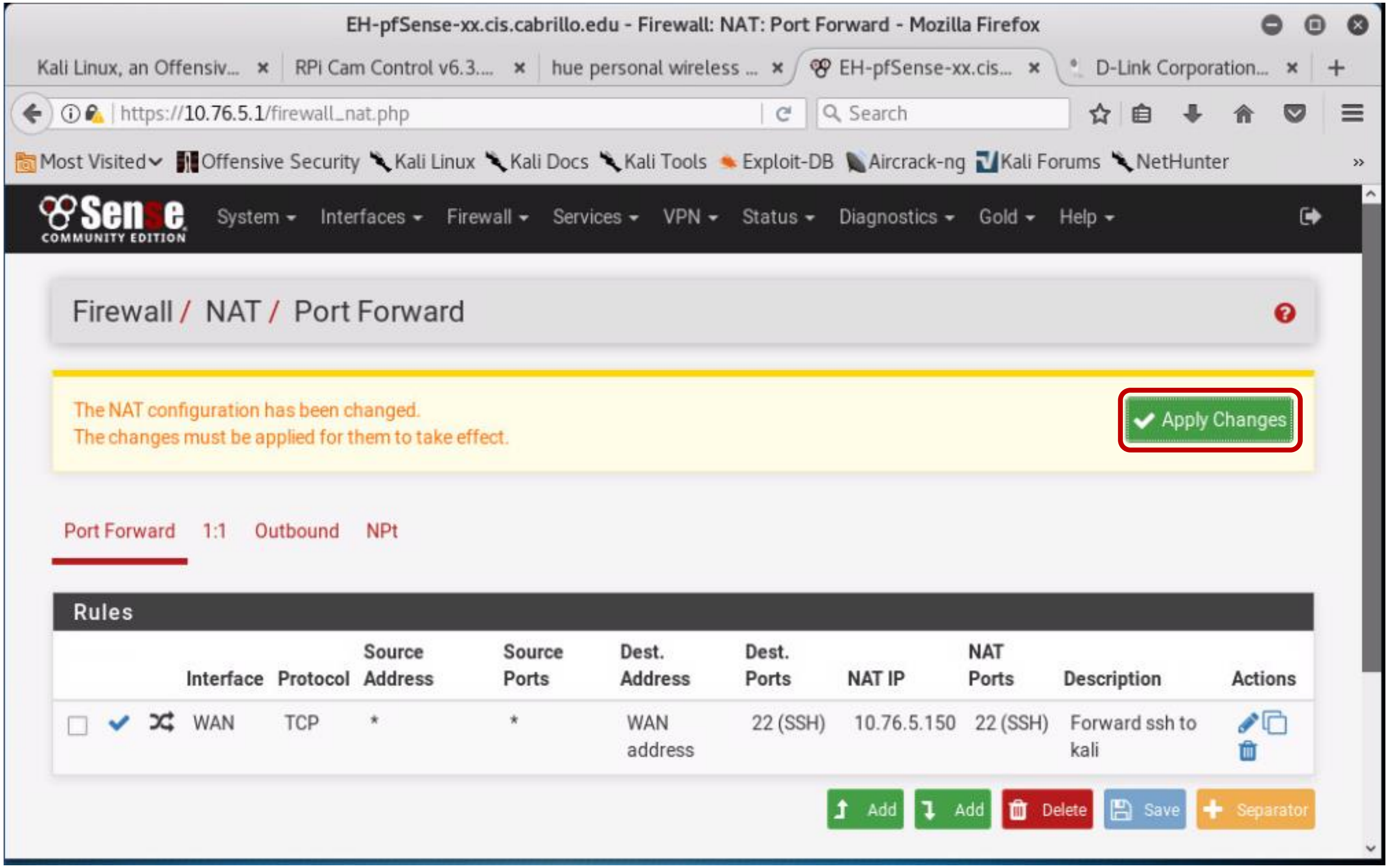
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

Description: Forward ssh to kali

A description may be entered here for administrative reference (not parsed).

Navigate to Firewall > NAT > select Port Forward "tab" > Click Add button then fill out the fields highlighted above. When finished click "Save" button at the bottom of the page.

Apply the new rule to your configuration



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

https://10.76.5.1/firewall_nat.php

Firewall / NAT / Port Forward

The NAT configuration has been changed.
The changes must be applied for them to take effect.

✔ Apply Changes

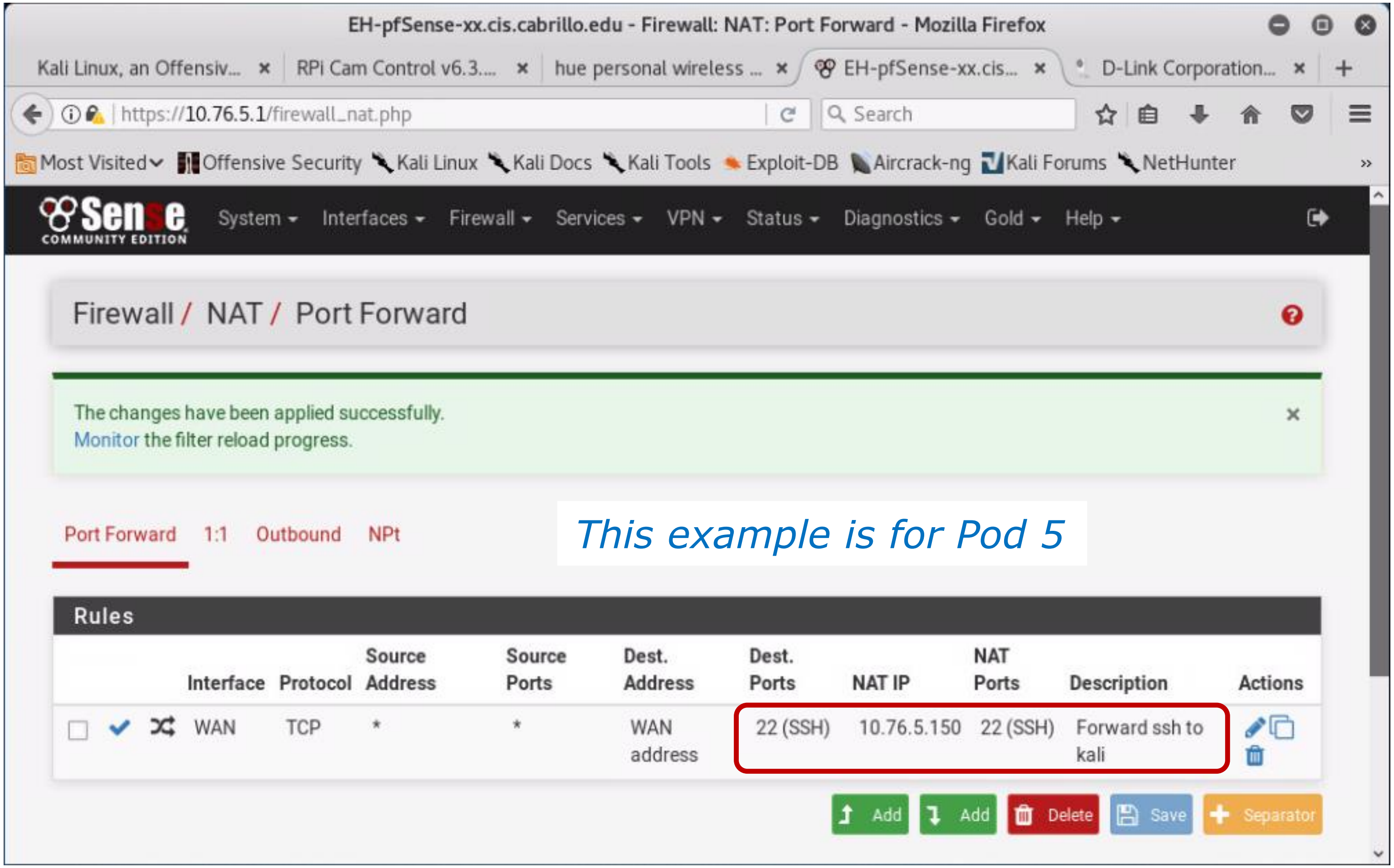
Port Forward | 1:1 | Outbound | NPt

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓		WAN	TCP	*	*	WAN address	22 (SSH)	10.76.5.150	22 (SSH)	Forward ssh to kali	

Click the Apply Changes button

Review the new NAT Port Forward Rule



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

https://10.76.5.1/firewall_nat.php

Firewall / NAT / Port Forward

The changes have been applied successfully.
Monitor the filter reload progress.

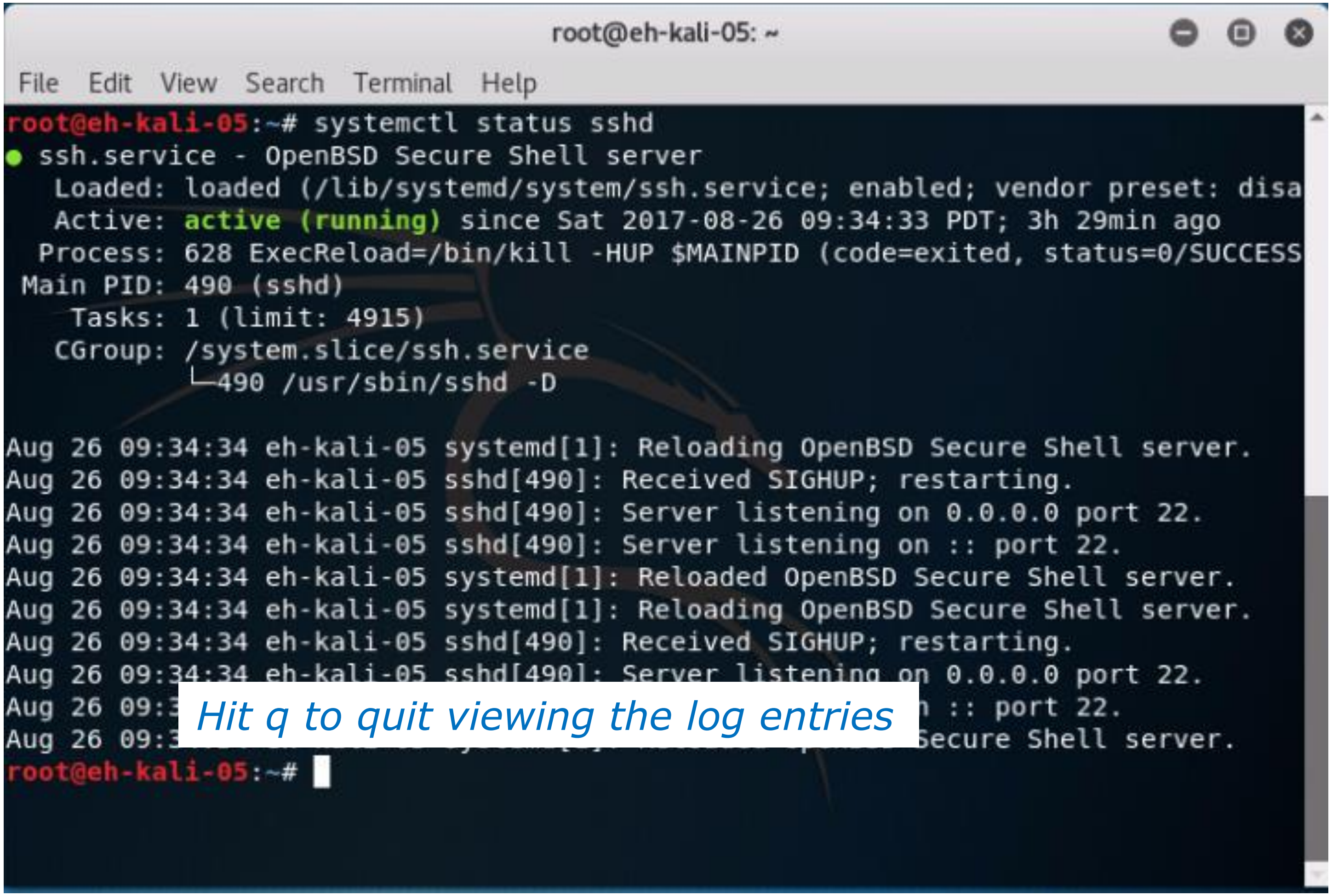
This example is for Pod 5

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⤮	WAN	TCP	*	*	WAN address	22 (SSH)	10.76.5.150	22 (SSH)	Forward ssh to kali	

Your IP and port should be 10.76.xx.150 port 22 where xx is your pod number.

Verifying ssh service on Kali is running

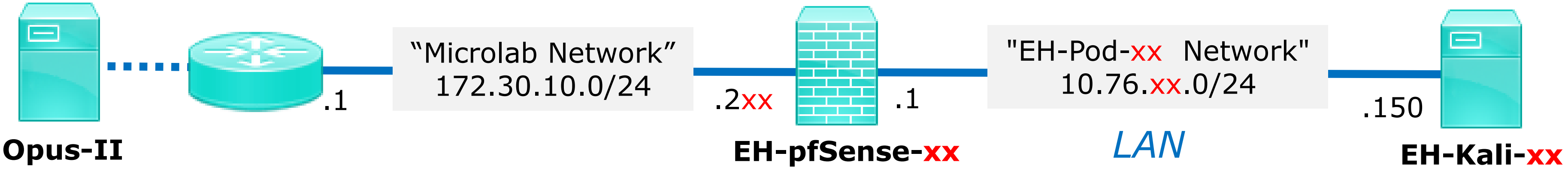


```
root@eh-kali-05:~# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disa
   Active: active (running) since Sat 2017-08-26 09:34:33 PDT; 3h 29min ago
  Process: 628 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS
 Main PID: 490 (sshd)
    Tasks: 1 (limit: 4915)
   CGroup: /system.slice/ssh.service
           └─490 /usr/sbin/sshd -D

Aug 26 09:34:34 eh-kali-05 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 26 09:34:34 eh-kali-05 sshd[490]: Received SIGHUP; restarting.
Aug 26 09:34:34 eh-kali-05 sshd[490]: Server listening on 0.0.0.0 port 22.
Aug 26 09:34:34 eh-kali-05 sshd[490]: Server listening on :: port 22.
Aug 26 09:34:34 eh-kali-05 systemd[1]: Reloaded OpenBSD Secure Shell server.
Aug 26 09:34:34 eh-kali-05 systemd[1]: Reloading OpenBSD Secure Shell server.
Aug 26 09:34:34 eh-kali-05 sshd[490]: Received SIGHUP; restarting.
Aug 26 09:34:34 eh-kali-05 sshd[490]: Server listening on 0.0.0.0 port 22.
Aug 26 09:3                                               n :: port 22.
Aug 26 09:3                                               Secure Shell server.
root@eh-kali-05:~#
```

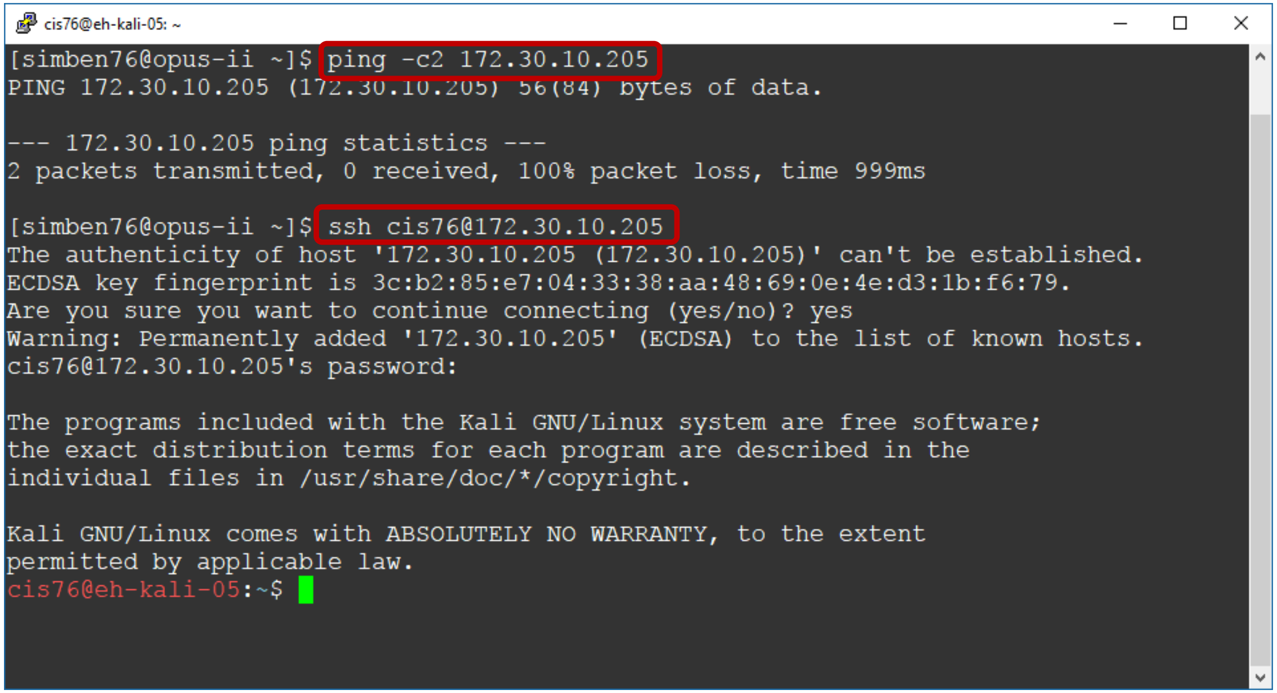
Hit q to quit viewing the log entries

If not running, start it with: **systemctl start sshd**

Testing port forwarding from Opus-II



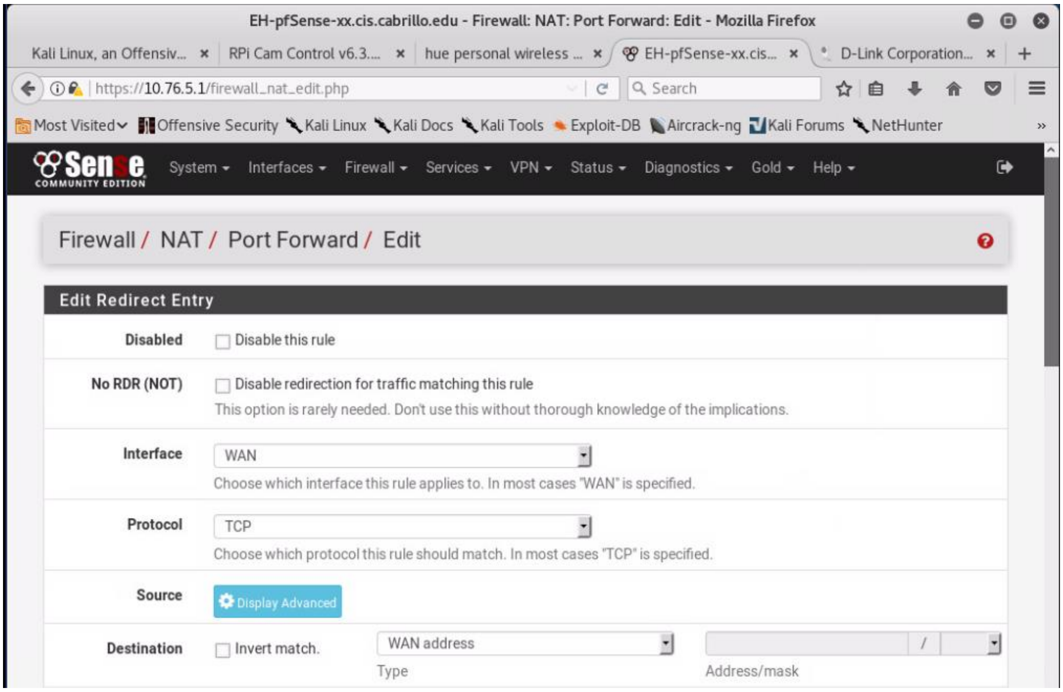
On Opus-II: ssh cis76@172.30.10.2xx



```
[simben76@opus-ii ~]$ ping -c2 172.30.10.205
PING 172.30.10.205 (172.30.10.205) 56(84) bytes of data.

--- 172.30.10.205 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms

[simben76@opus-ii ~]$ ssh cis76@172.30.10.205
The authenticity of host '172.30.10.205 (172.30.10.205)' can't be established.
ECDSA key fingerprint is 3c:b2:85:e7:04:33:38:aa:48:69:0e:4e:d3:1b:f6:79.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.30.10.205' (ECDSA) to the list of known hosts.
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.
cis76@eh-kali-05:~$
```

Note, the firewall on your pfSense VM will block pings but allow and forward ssh traffic to your Kali VM

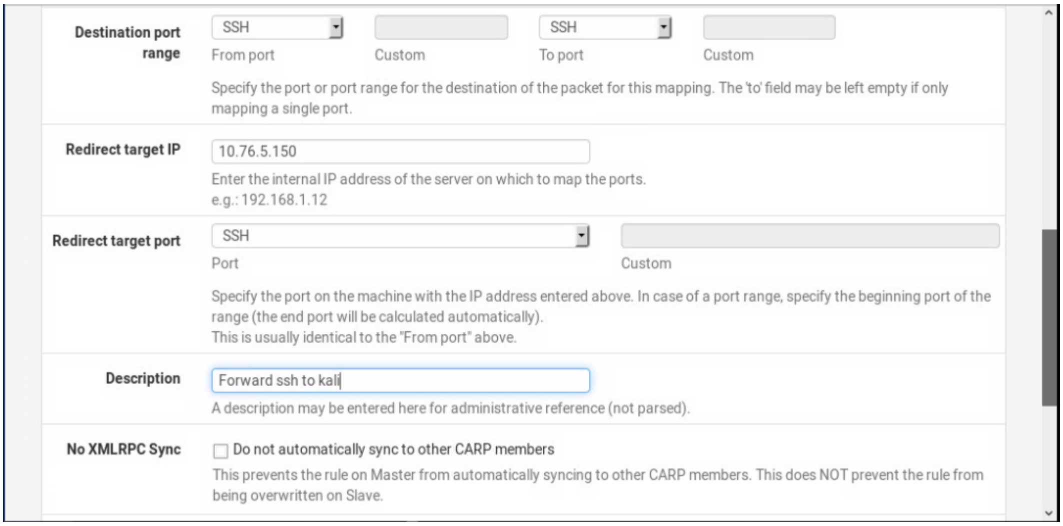
Pod 5 Reference Example



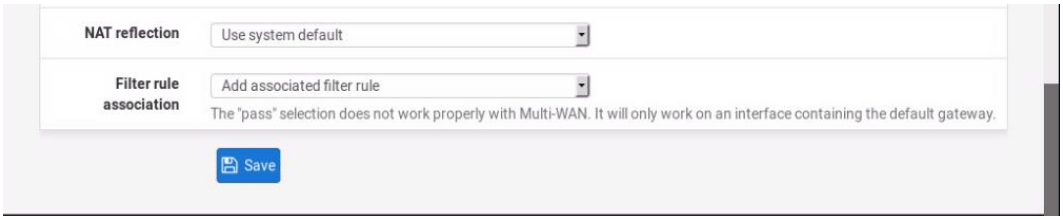
Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

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 Choose which interface this rule applies to. In most cases "WAN" is specified.
Protocol	TCP Choose which protocol this rule should match. In most cases "TCP" is specified.
Source	Display Advanced
Destination	□ Invert match. WAN address (Type) / Address/mask



Destination port range	SSH (From port) Custom; SSH (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 (Port) Custom Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.
Description	Forward ssh to kali A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync	□ Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.



NAT reflection	Use system default
Filter rule association	Add associated filter rule The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

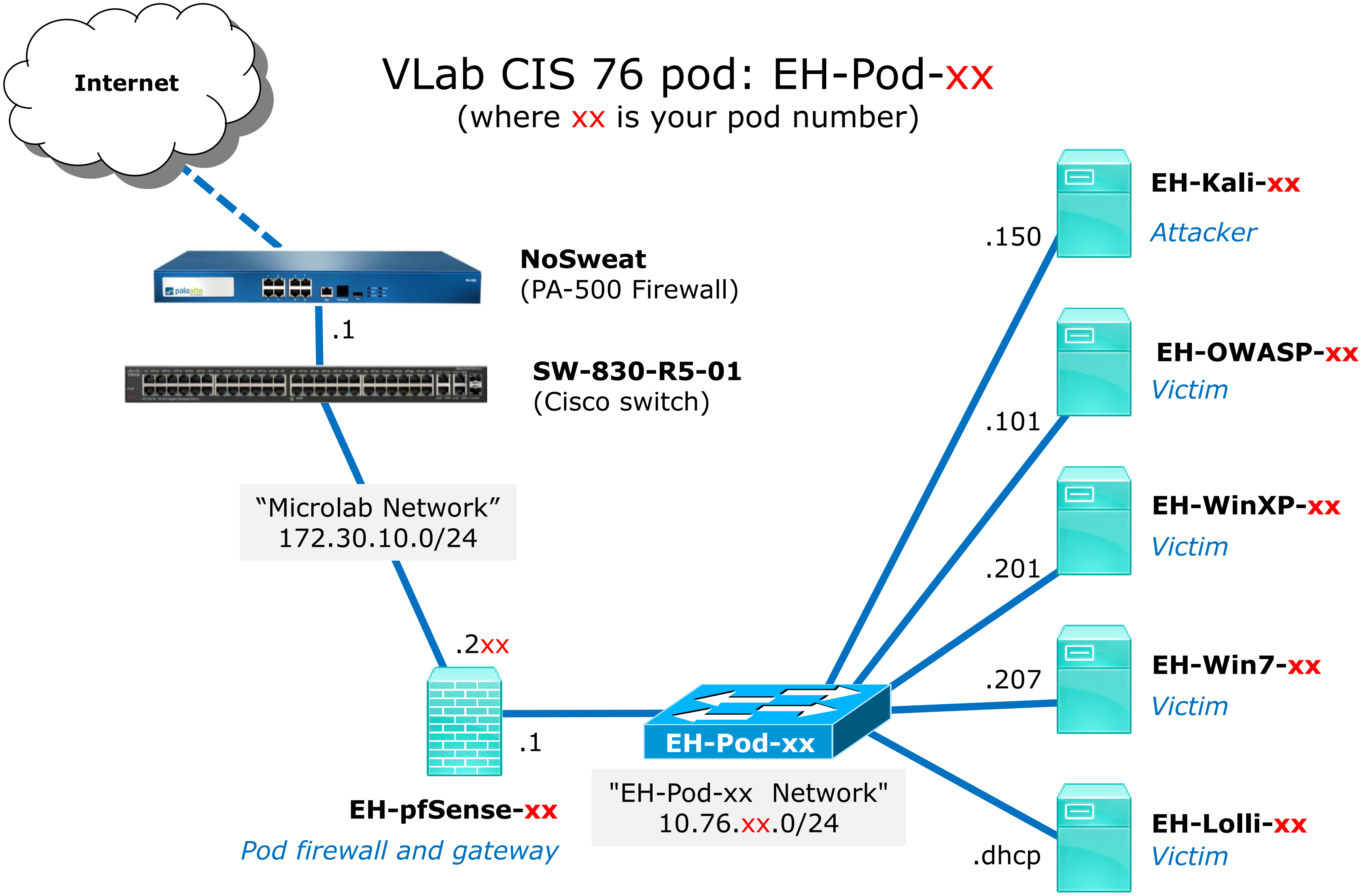
Save

Repeat of previous slides show full view of new rule added (zoom to see).

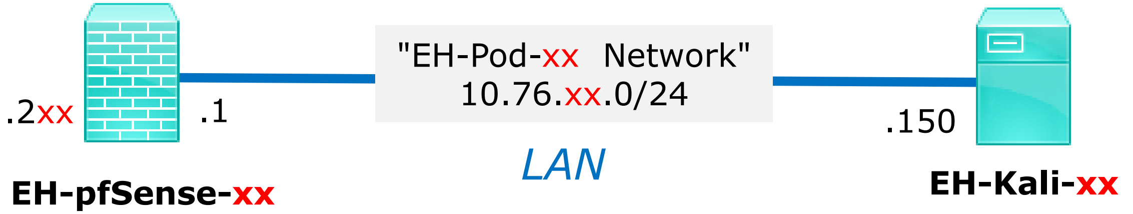
EH-Kali-xx VM Config

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



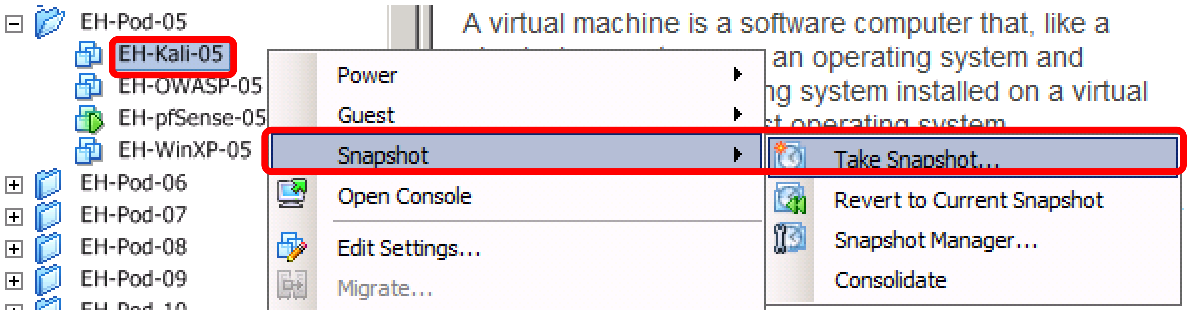
Configuring the EH-Kali VM in EH-Pod-xx



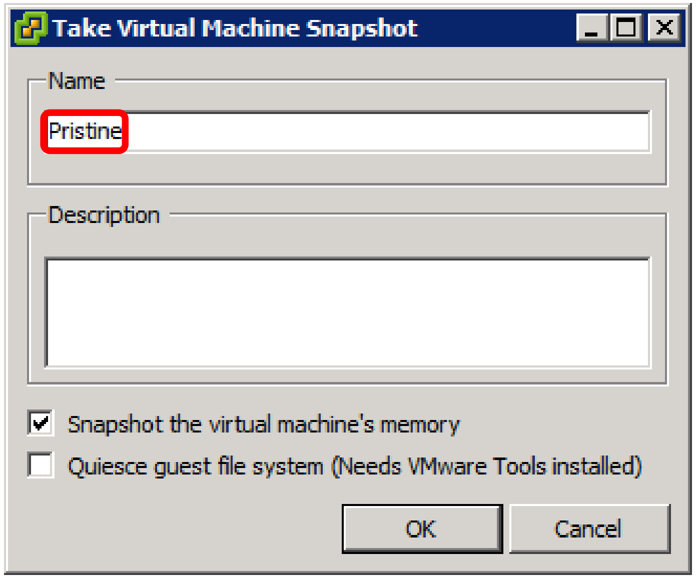
xx is the pod number assigned to you.

Kali VM	Pod xx settings
VM Network Adapter 1	EH-Pod-xx Net
Hostname	EH-Kali-xx
IPv4 address	10.76.xx.150
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.xx.1
Primary name server	172.30.5.101
Secondary name server	172.30.5.102
Domain search string	cis.cabrillo.edu
sshd service	started and enabled

Configuring the EH-Kali VM in EH-Pod-xx



Pod 5 example



Name: Pristine

Description:

☑ Snapshot the virtual machine's memory

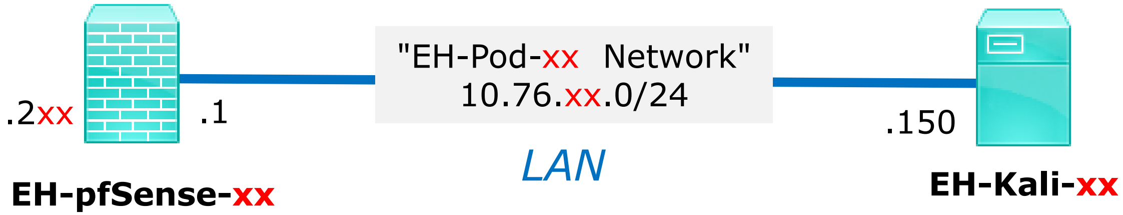
☐ Quiesce guest file system (Needs VMware Tools installed)

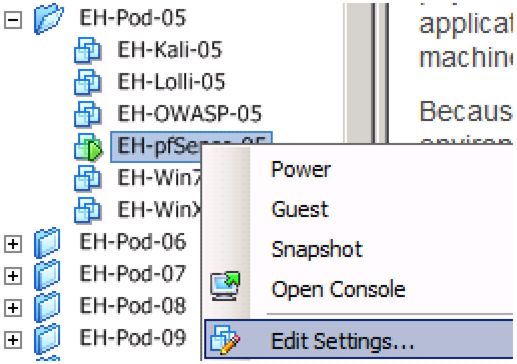
IMPORTANT, back up your VM!

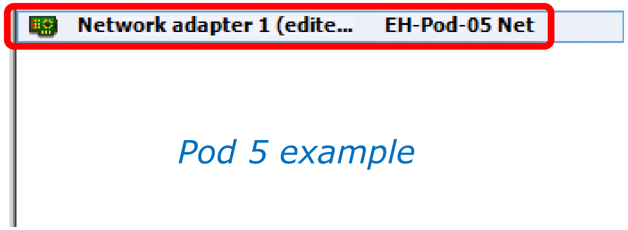
1) Make a backup snapshot of your Kali VM named "**Pristine**".

Now if you mess things up you can always start over again!

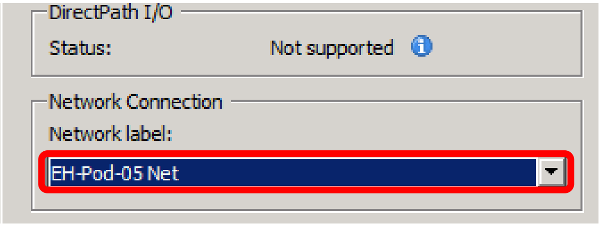
Configuring the EH-Kali VM in EH-Pod-xx






Network adapter 1 (edite... EH-Pod-05 Net

Pod 5 example


DirectPath I/O

Status: Not supported

Network Connection

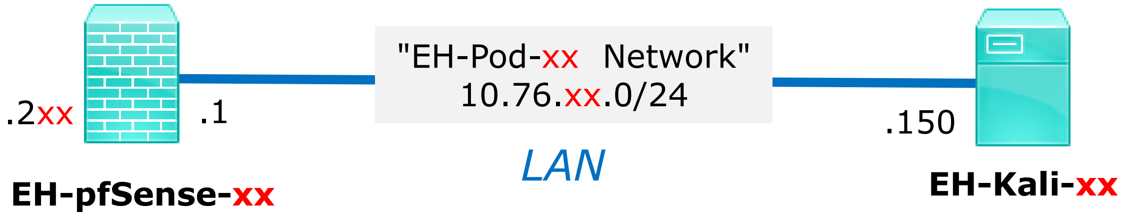
Network label: EH-Pod-05 Net

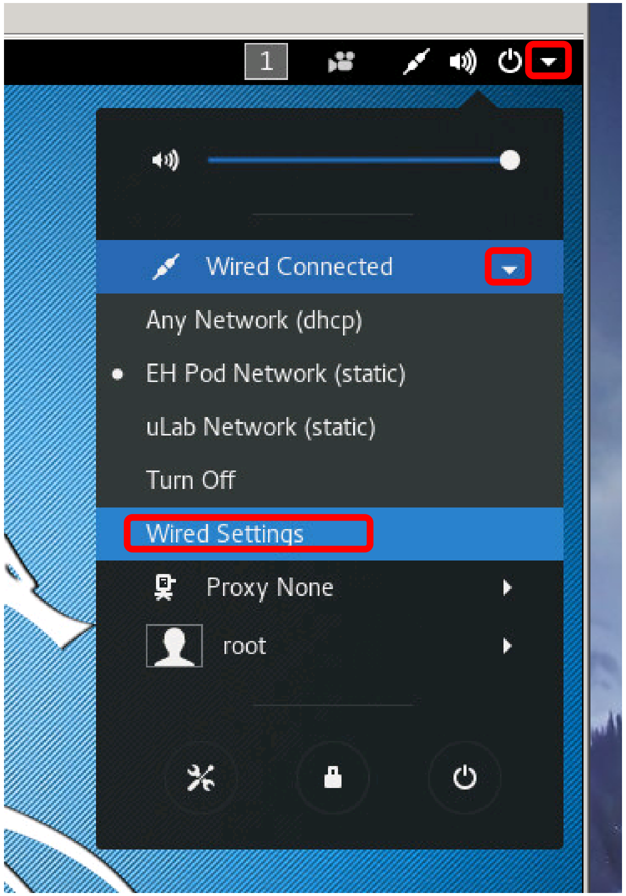
Network Cabling

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.

Configuring the EH-Kali VM in EH-Pod-xx





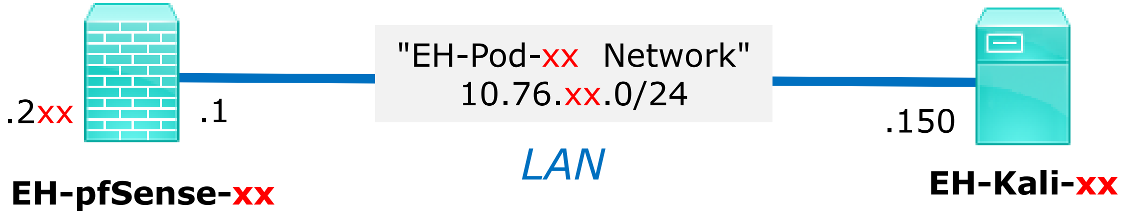
Network Configuration

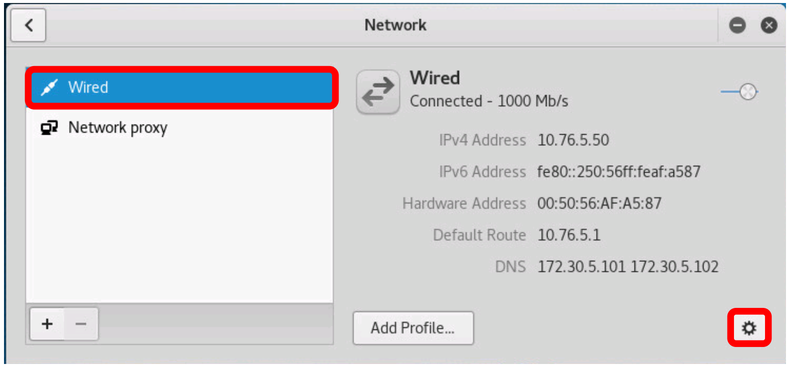
1) Power up the VM and open a console.

2) Login as the root user.

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

Configuring the EH-Kali VM in EH-Pod-xx



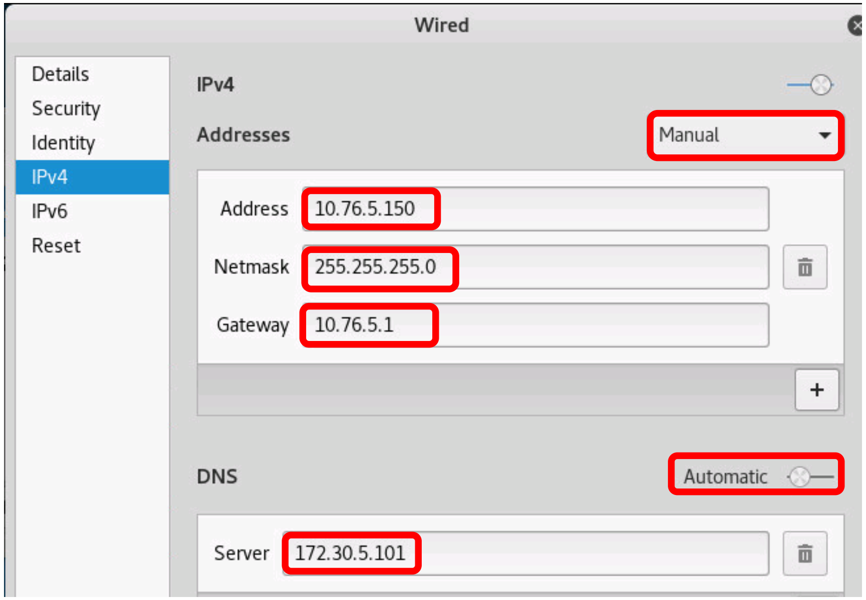

Network

Wired
Network proxy

Wired
Connected - 1000 Mb/s

IPv4 Address	10.76.5.50
IPv6 Address	fe80::250:56ff:feaf:a587
Hardware Address	00:50:56:AF:A5:87
Default Route	10.76.5.1
DNS	172.30.5.101 172.30.5.102

Pod 5 example


Wired

IPv4

Addresses: Manual

Address: 10.76.5.150

Netmask: 255.255.255.0

Gateway: 10.76.5.1

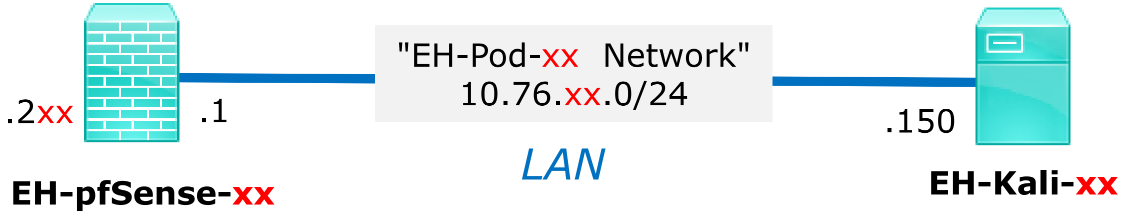
DNS: Automatic

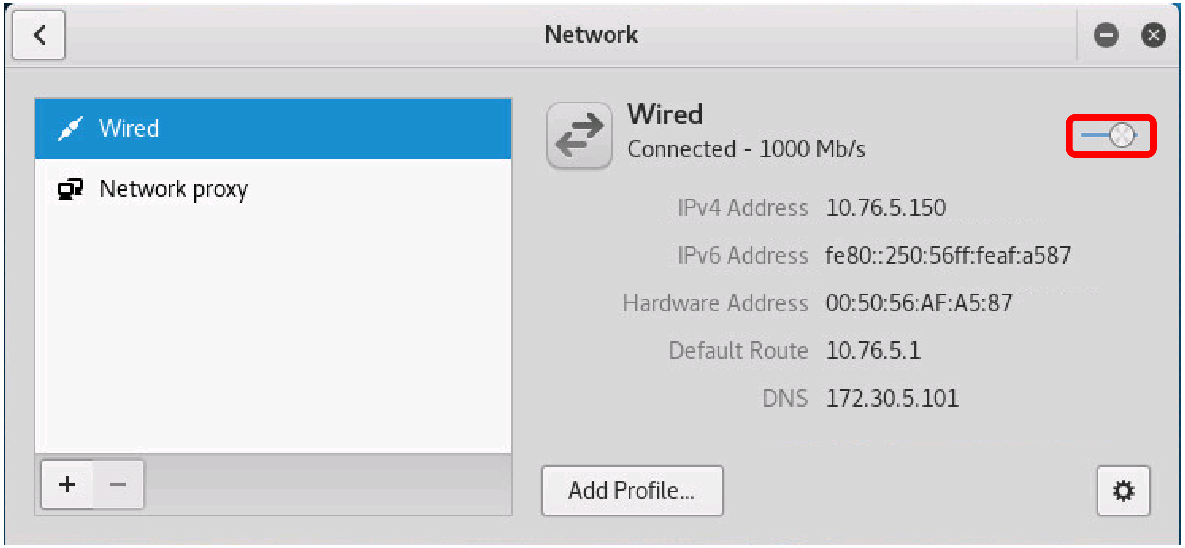
Server: 172.30.5.101

4) Click the gear icon for the "Wired" profile.

5) For IPv4 tab update the Address with 10.76.xx.150, the Netmask with 255.255.255.0, the Gateway with 10.76.xx.1 and the DNS Server with 172.30.5.101, where xx is your pod number. Then click Apply button.

Configuring the EH-Kali VM in EH-Pod-xx





Wired
Connected - 1000 Mb/s

IPv4 Address 10.76.5.150

IPv6 Address fe80::250:56ff:feaf:a587

Hardware Address 00:50:56:AF:A5:87

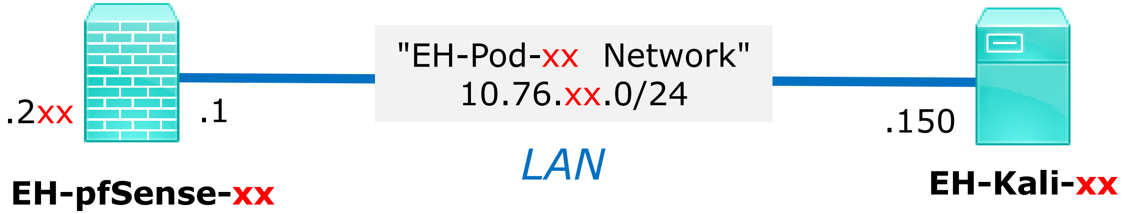
Default Route 10.76.5.1

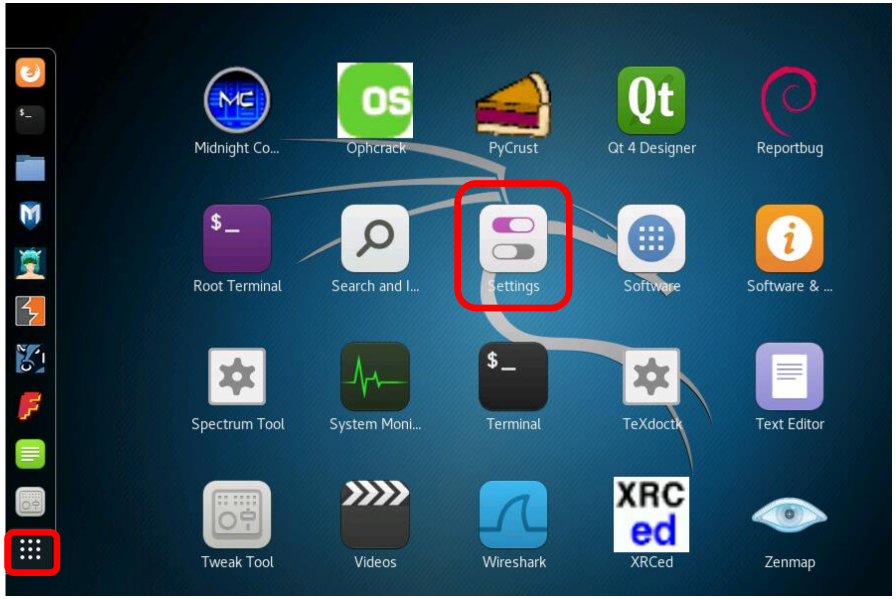
DNS 172.30.5.101

Pod 5 example

6) Click on the Wired profile and toggle the interface off and on again. Make sure you see the updated IPv4 address and Default Route for <u>your</u> pod (not Pod 5). Then close the Network dialog box.

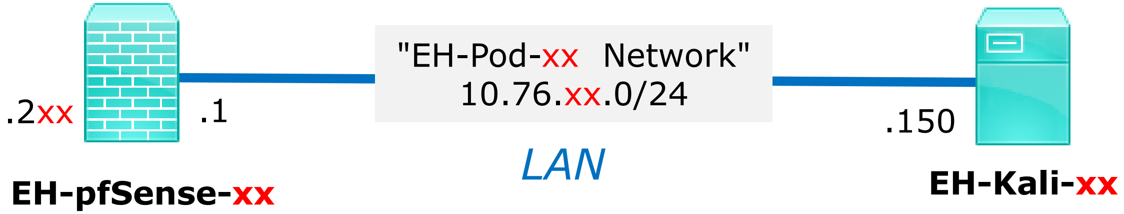
Configuring the EH-Kali VM in EH-Pod-xx

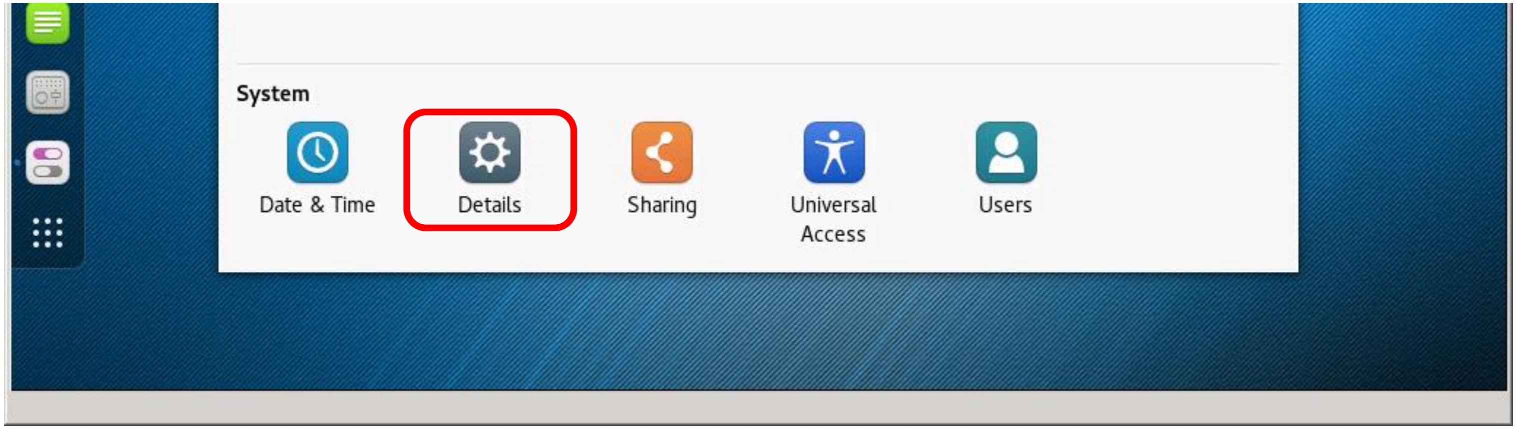




7) Show the applications, scroll down and open the Settings icon.

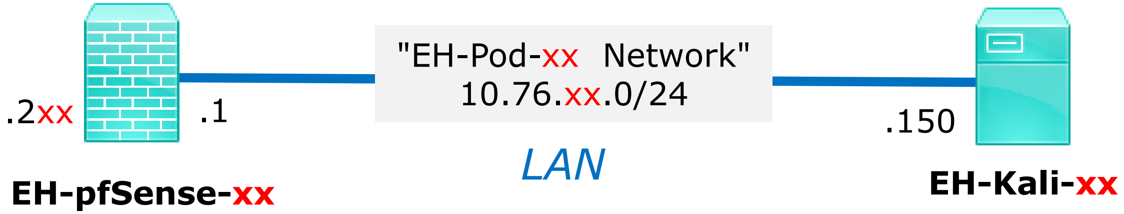
Configuring the EH-Kali VM in EH-Pod-xx





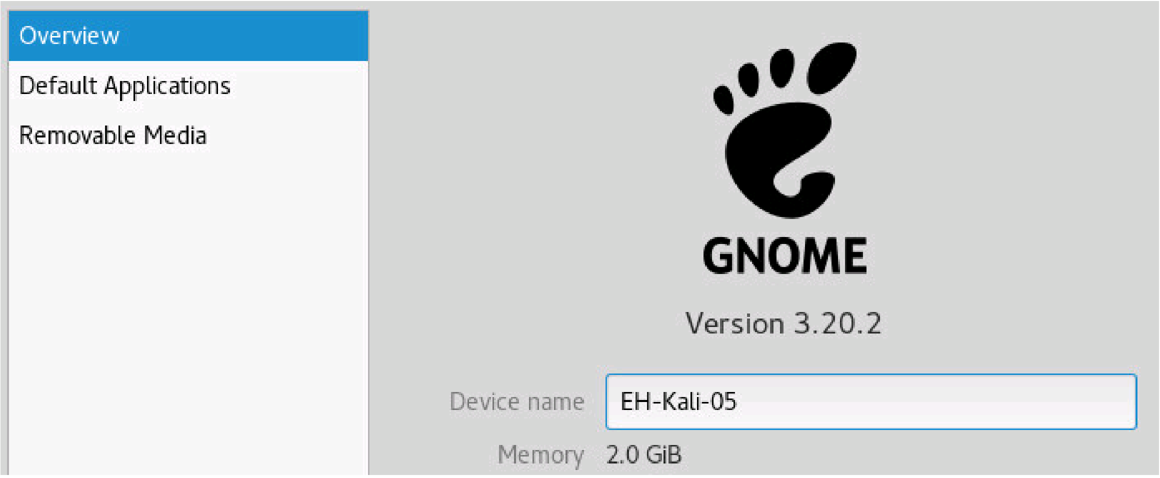
8) Open the Details icon in the All Settings dialog box.

Configuring the EH-Kali VM in EH-Pod-xx



This example shows pod 5.

Each student should only use the pod assigned to them.



Version 3.20.2

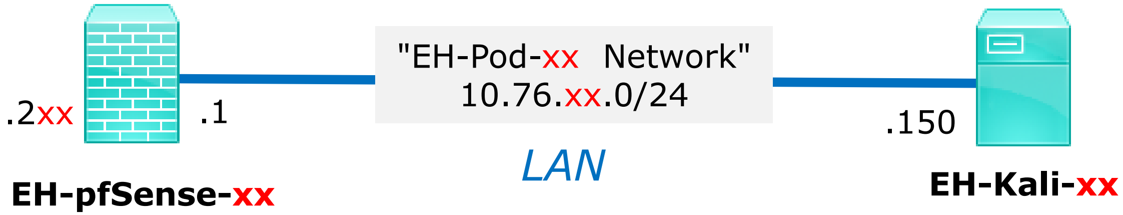
Device name: EH-Kali-05

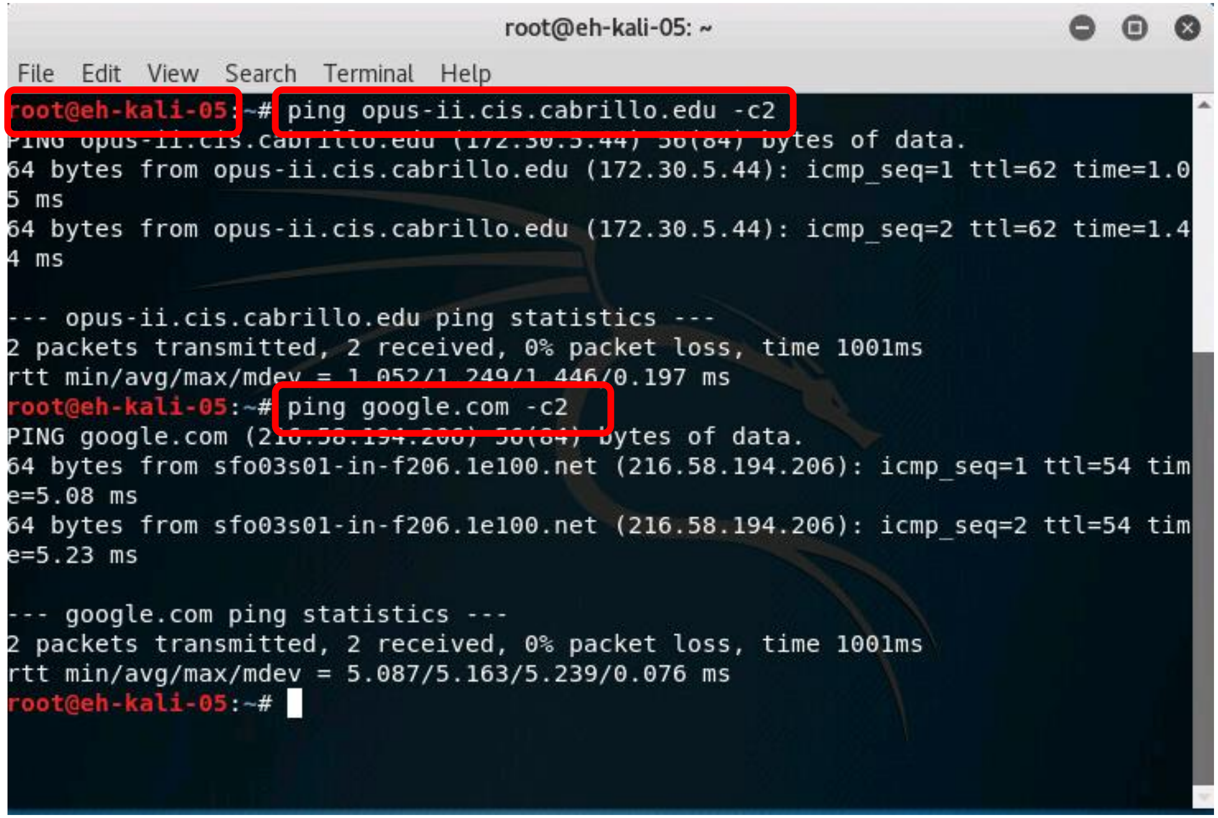
Memory: 2.0 GiB

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

10) Close the dialog box.

Configuring the EH-Kali VM in EH-Pod-xx



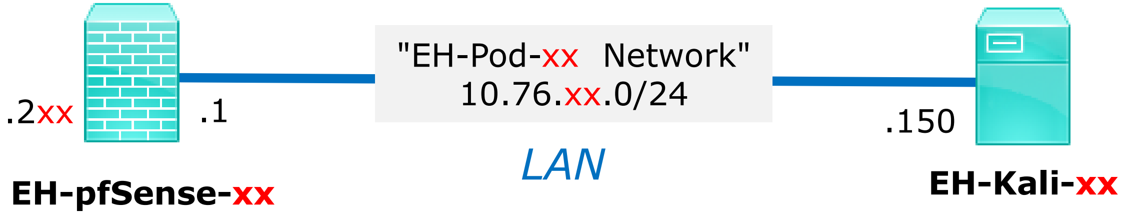


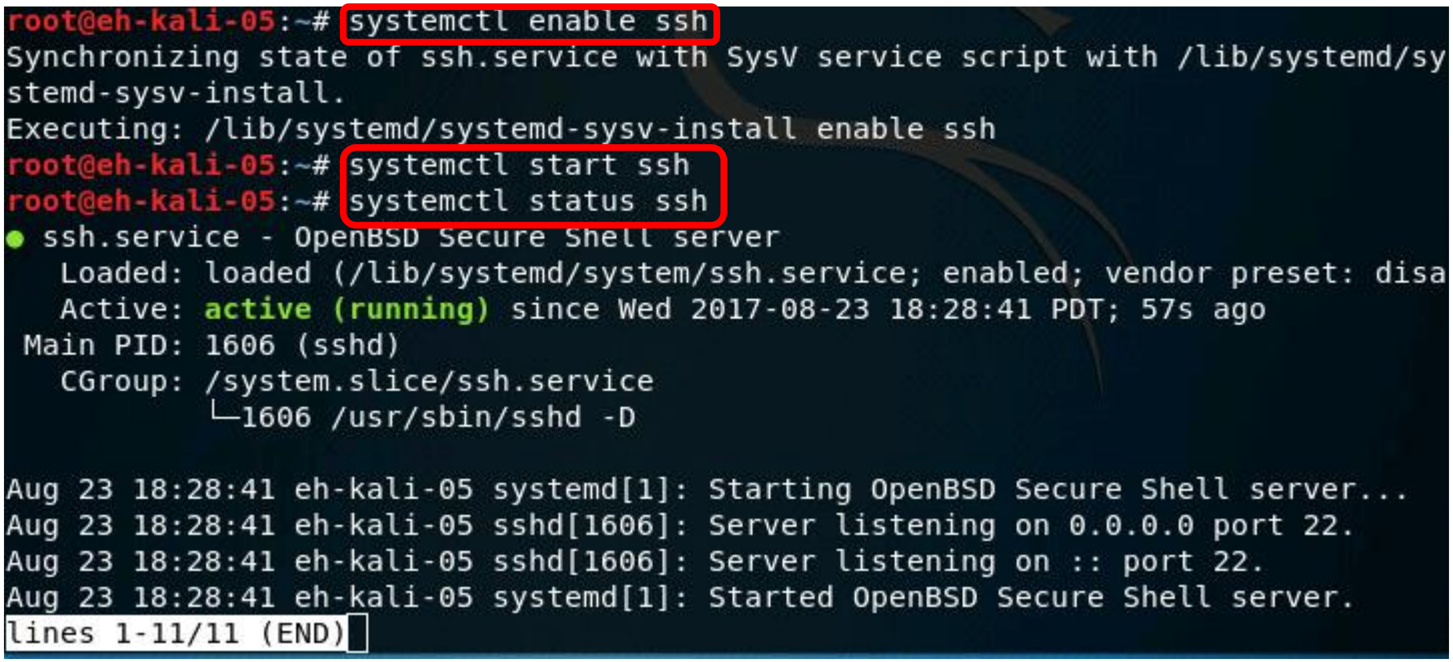
```
root@eh-kali-05:~# ping opus-ii.cis.cabrillo.edu -c2
PING opus-ii.cis.cabrillo.edu (172.30.5.44) 56(84) bytes of data.
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=1 ttl=62 time=1.0
5 ms
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=2 ttl=62 time=1.4
4 ms

--- opus-ii.cis.cabrillo.edu ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.052/1.249/1.446/0.197 ms
root@eh-kali-05:~# ping google.com -c2
PING google.com (216.58.194.206) 56(84) bytes of data.
64 bytes from sfo03s01-in-f206.1e100.net (216.58.194.206): icmp_seq=1 ttl=54 tim
e=5.08 ms
64 bytes from sfo03s01-in-f206.1e100.net (216.58.194.206): icmp_seq=2 ttl=54 tim
e=5.23 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 5.087/5.163/5.239/0.076 ms
root@eh-kali-05:~# 
```

10) Bring up a terminal and verify the prompt "root@kali-xx" and you can ping Opus-II and Google.

Note, your pfSense VM must be configured and running or your pings will fail!

Configuring the EH-Kali VM in EH-Pod-xx

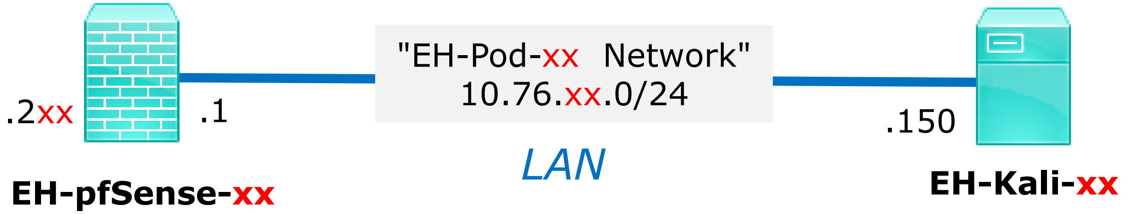


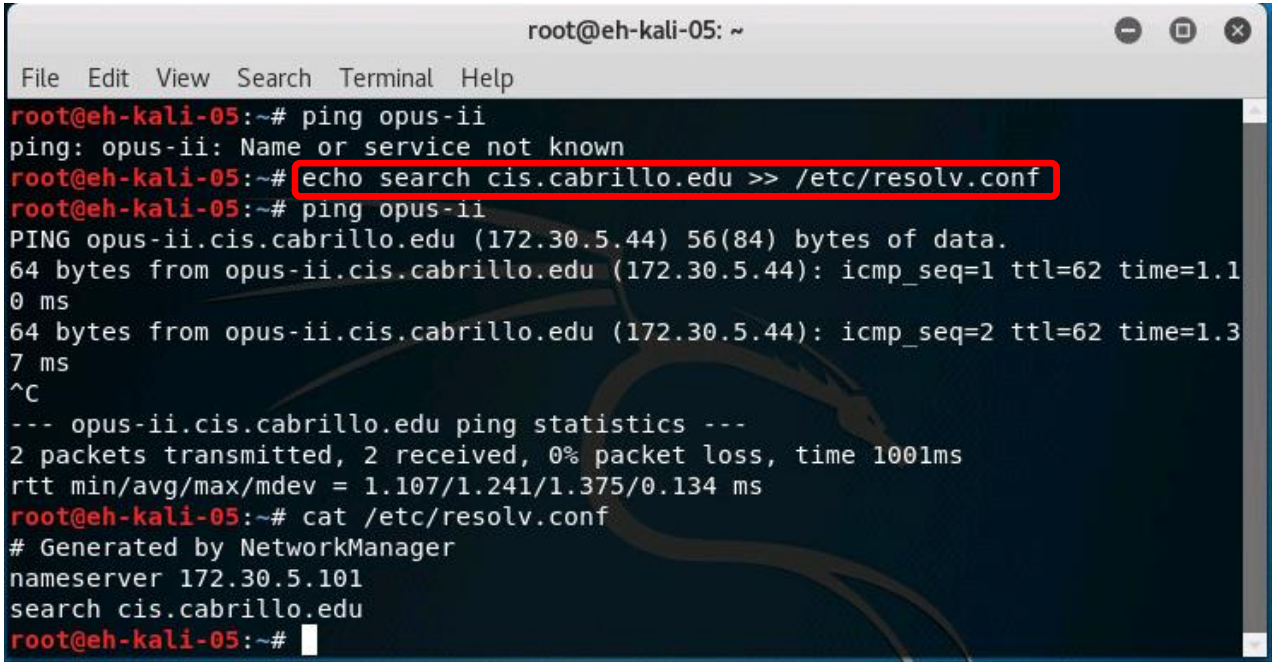


```
root@eh-kali-05:~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
root@eh-kali-05:~# systemctl start ssh
root@eh-kali-05:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disa
   Active: active (running) since Wed 2017-08-23 18:28:41 PDT; 57s ago
 Main PID: 1606 (sshd)
   CGroup: /system.slice/ssh.service
           └─1606 /usr/sbin/sshd -D

Aug 23 18:28:41 eh-kali-05 systemd[1]: Starting OpenBSD Secure Shell server...
Aug 23 18:28:41 eh-kali-05 sshd[1606]: Server listening on 0.0.0.0 port 22.
Aug 23 18:28:41 eh-kali-05 sshd[1606]: Server listening on :: port 22.
Aug 23 18:28:41 eh-kali-05 systemd[1]: Started OpenBSD Secure Shell server.
lines 1-11/11 (END)
```

11) Enable ssh to start automatically on boot. Then start it and check status. Hit "q" exit the status listing.

Configuring the EH-Kali VM in EH-Pod-xx

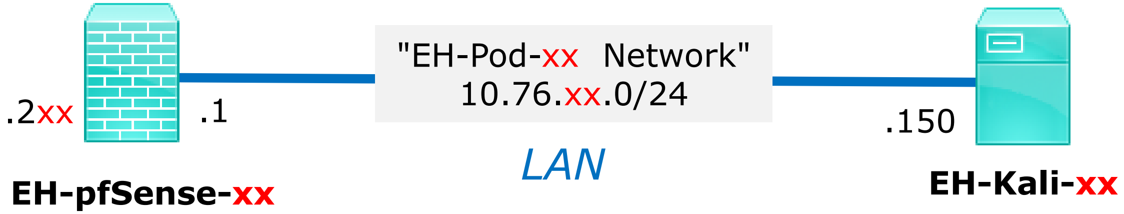




```
root@eh-kali-05:~# ping opus-ii
ping: opus-ii: Name or service not known
root@eh-kali-05:~# echo search cis.cabrillo.edu >> /etc/resolv.conf
root@eh-kali-05:~# ping opus-ii
PING opus-ii.cis.cabrillo.edu (172.30.5.44) 56(84) bytes of data.
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=1 ttl=62 time=1.1
0 ms
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=2 ttl=62 time=1.3
7 ms
^C
--- opus-ii.cis.cabrillo.edu ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.107/1.241/1.375/0.134 ms
root@eh-kali-05:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 172.30.5.101
search cis.cabrillo.edu
root@eh-kali-05:~# 
```

12 You can add a DNS search string to /etc/resolv.conf if you would like to use short hostnames. However it won't be there after your next restart.

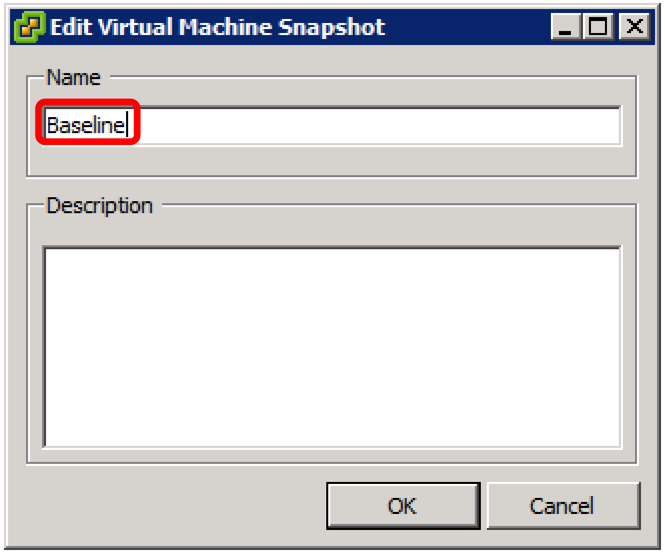
Configuring the EH-Kali VM in EH-Pod-xx



Save your work

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

Now if you mess things up later can always start over again!



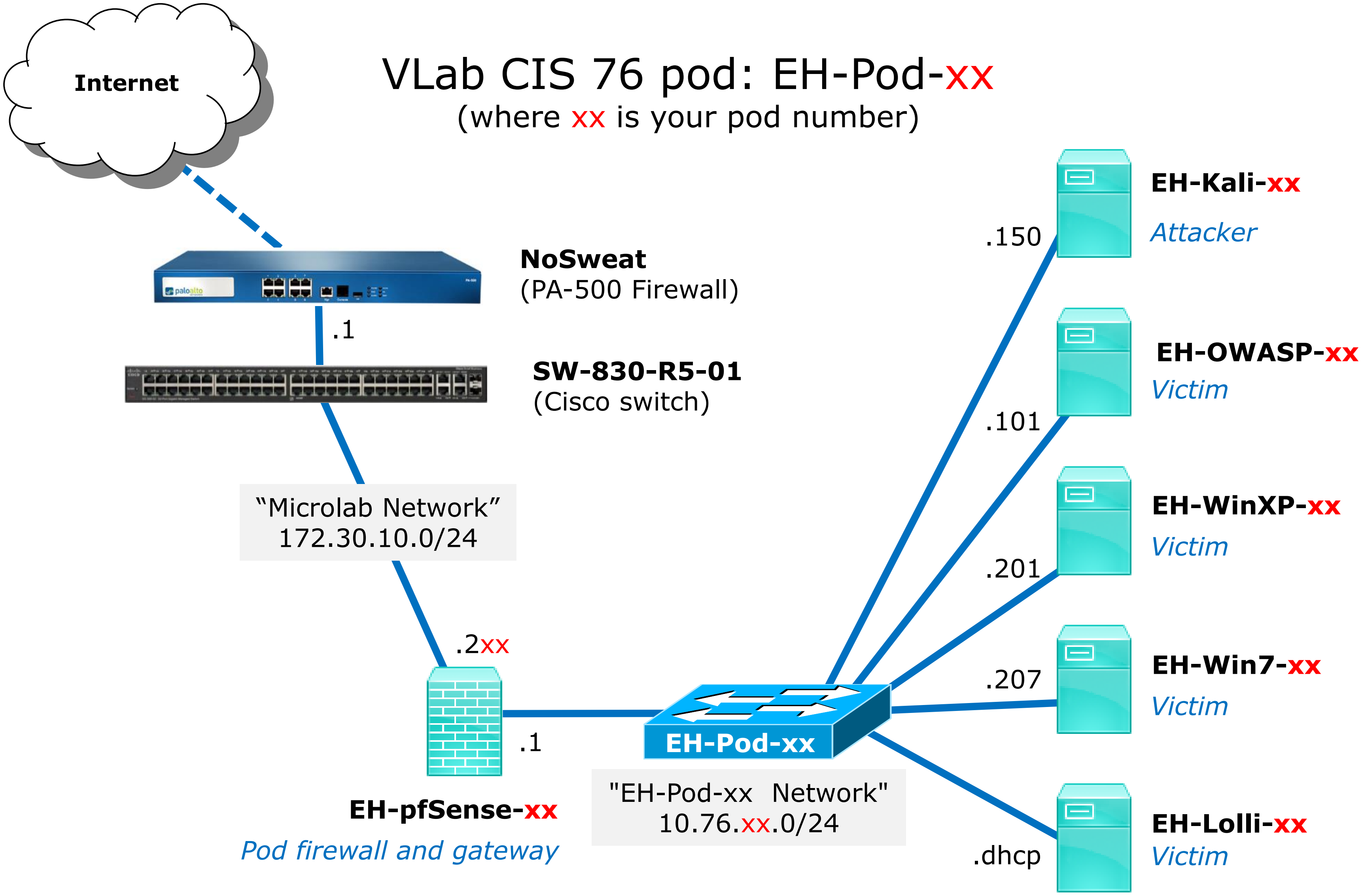
Name: Baseline

EH-WinXP VM Config

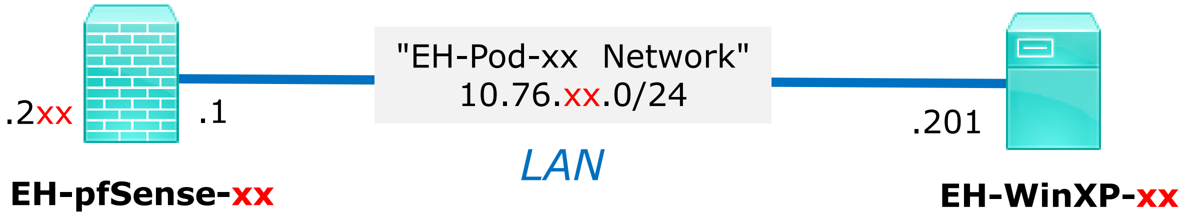
CIS 76 - VLab Pod Setup

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



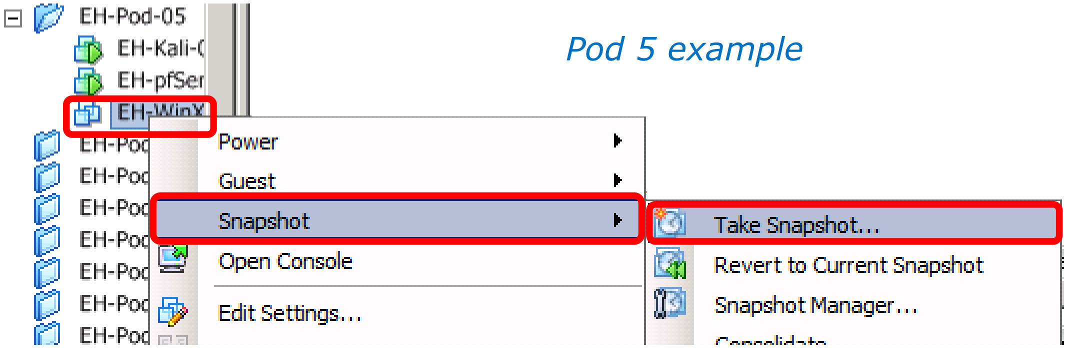
Configuring the EH-WinXP VM in EH-Pod-xx



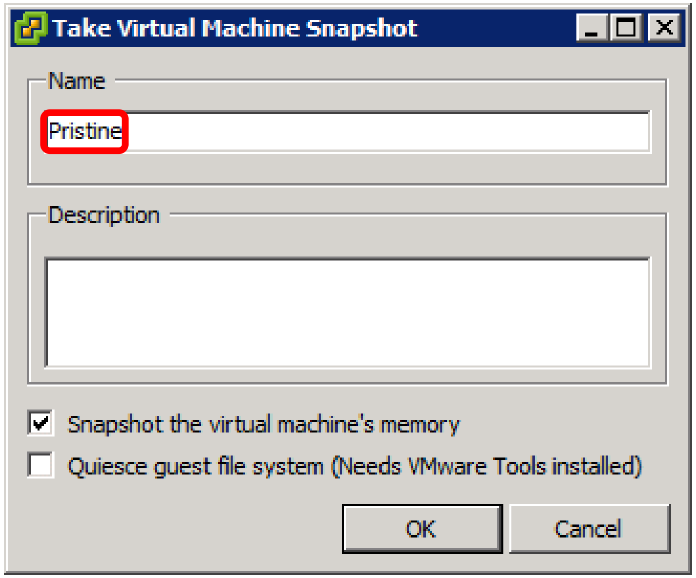
xx is the pod number assigned to you.

WinXP VM	Pod xx settings
VM Network Adapter 1	EH-Pod-xx Net
Computer Name	EH-WinXP-xx
IPv4 address	10.76.xx.201
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.xx.1
Preferred DNS server	172.30.5.101
Alternate DNS server	172.30.5.102
Domain suffix	cis.cabrillo.edu

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



Pod 5 example



Name

Pristine

Description

☑ Snapshot the virtual machine's memory

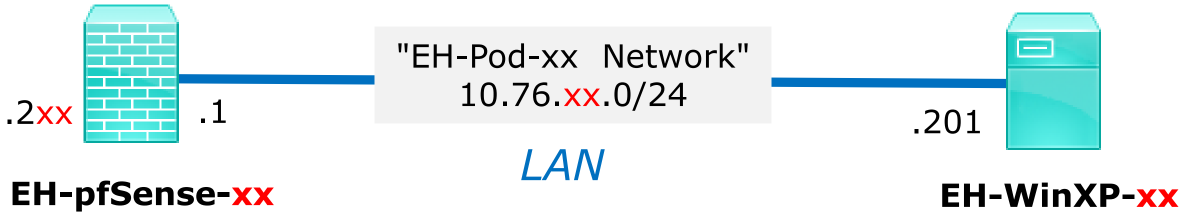
□ Quiesce guest file system (Needs VMware Tools installed)

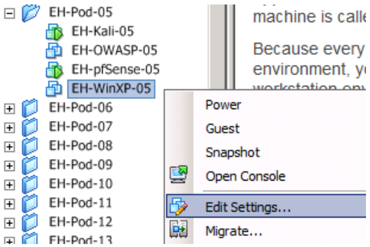
IMPORTANT, back up your VM!

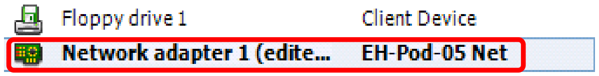
1) Make a backup snapshot of your WinXP VM named "**Pristine**".

Now if you mess things up you can always start over again!

Configuring the EH-WinXP VM in EH-Pod-xx

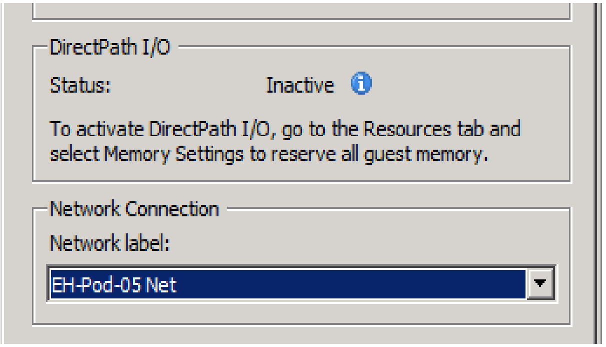





Floppy drive 1 Client Device

Network adapter 1 (edite... EH-Pod-05 Net

Pod 5 example


DirectPath I/O

Status: Inactive

To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory.

Network Connection

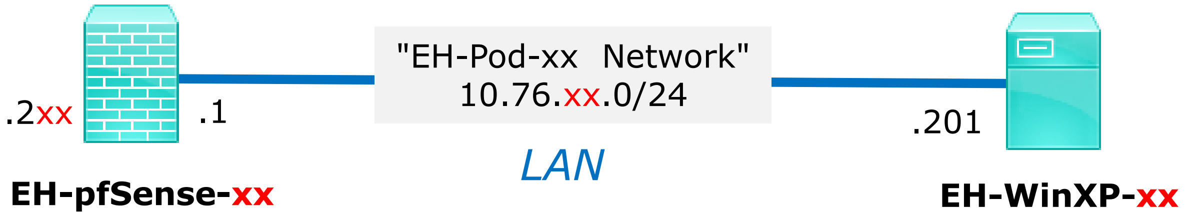
Network label: EH-Pod-05 Net

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.

Configuring the EH-WinXP VM in EH-Pod-xx

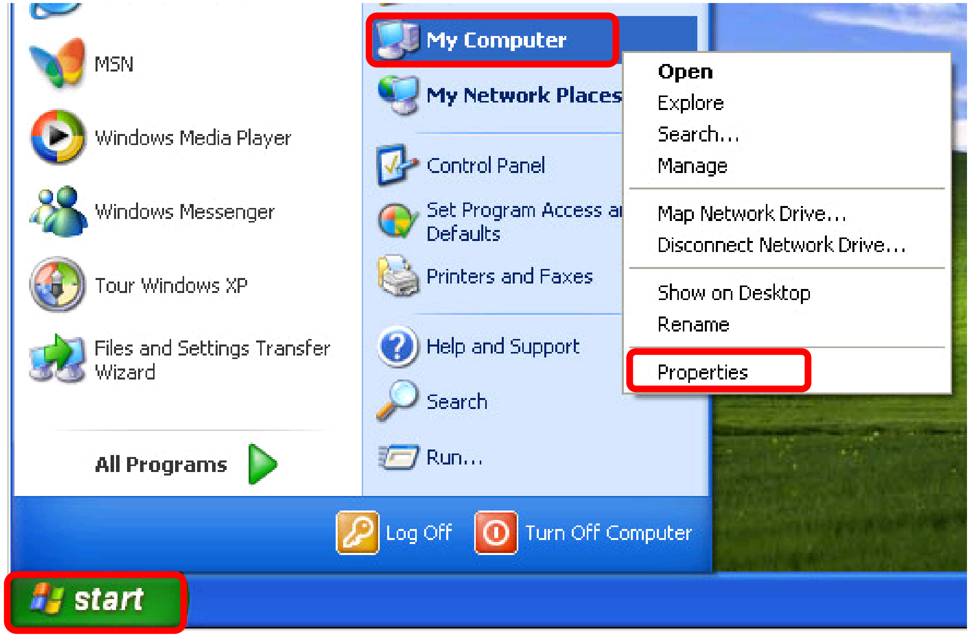


Computer Name Configuration

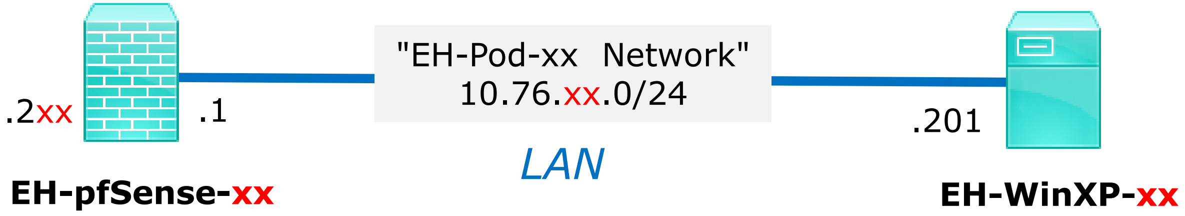
1) Power up the VM and open a console.

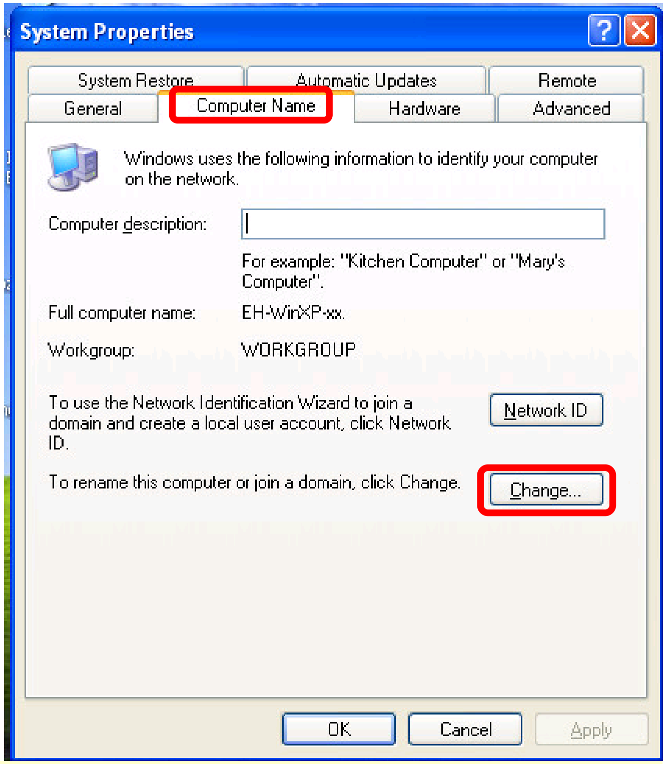
2) After initial setup has finished, login as the cis76 student user.

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



Configuring the EH-WinXP VM in EH-Pod-xx




System Properties

Tabs: System Restore | Automatic Updates | Remote | General | Computer Name | Hardware | Advanced

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

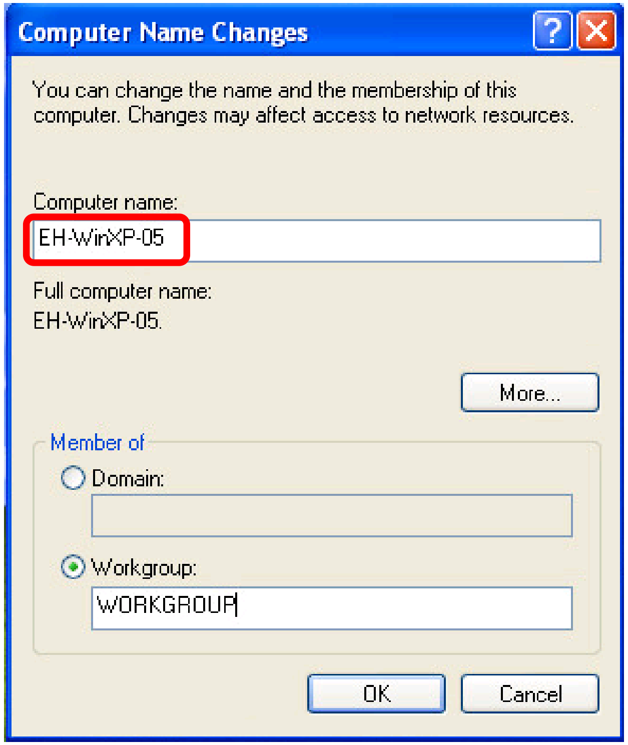
Full computer name: EH-WinXP-xx.

Workgroup: WORKGROUP

To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.

To rename this computer or join a domain, click Change.

4) Click the Computer Name tab then click Change.


Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: EH-WinXP-05

Full computer name:
EH-WinXP-05.

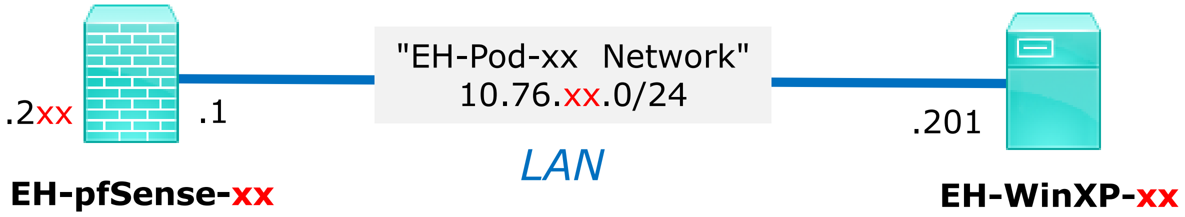
Member of

○ Domain:

● Workgroup: WORKGROUP

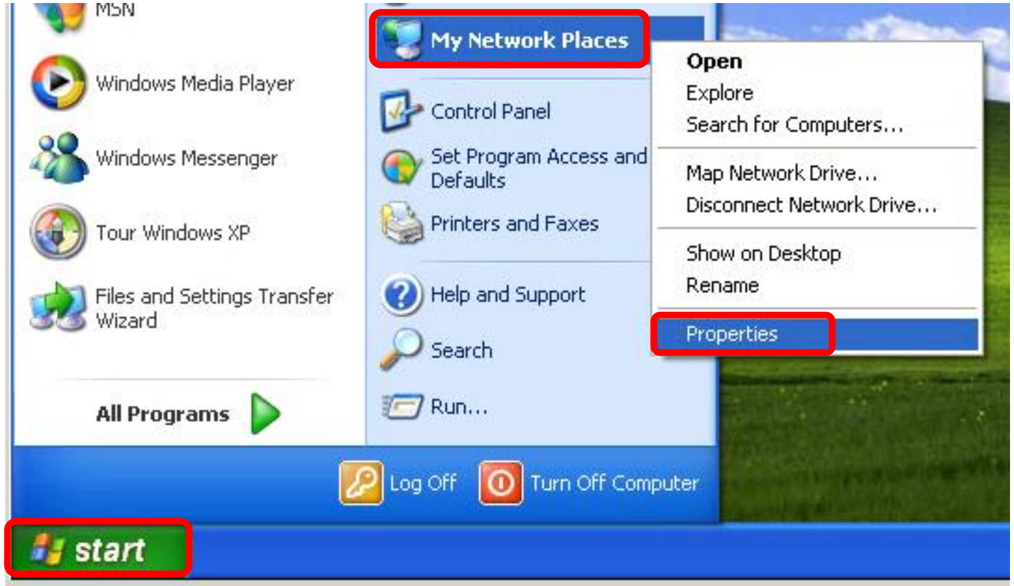
5) Update the Computer name with your two digit pod number xx. Click Ok and restart the VM.

Configuring the EH-WinXP VM in EH-Pod-xx

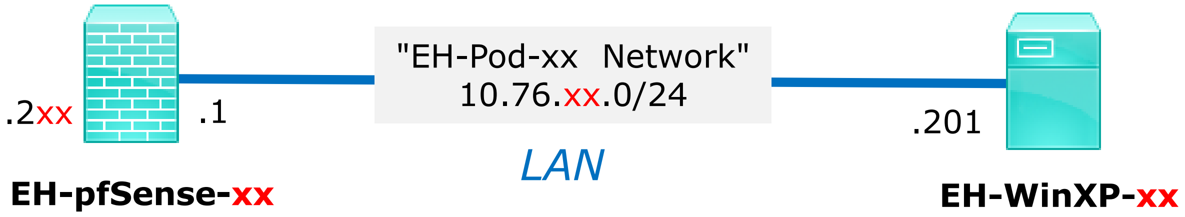


Network Configuration

1) Login again, click Start, right-click on "My Network Places" and Select Properties.



Configuring the EH-WinXP VM in EH-Pod-xx

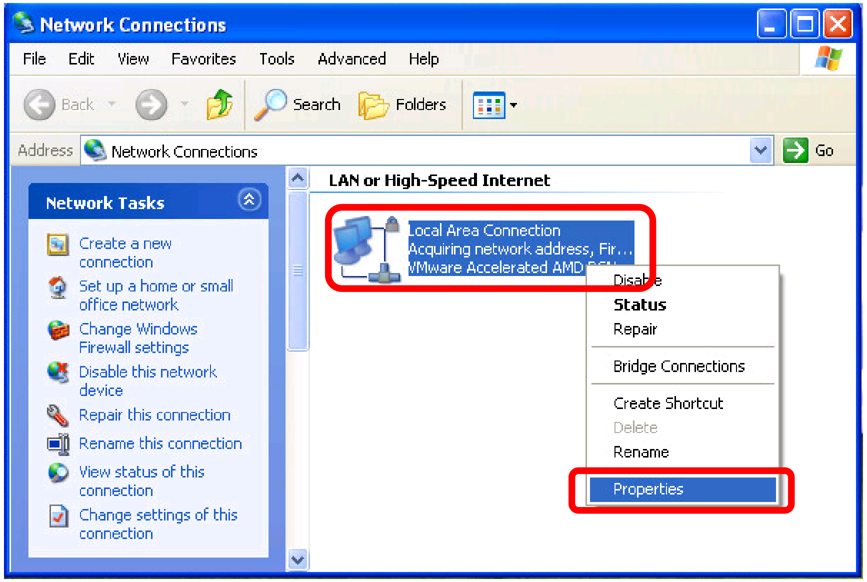


.2xx .1 "EH-Pod-xx Network" 10.76.xx.0/24 .201

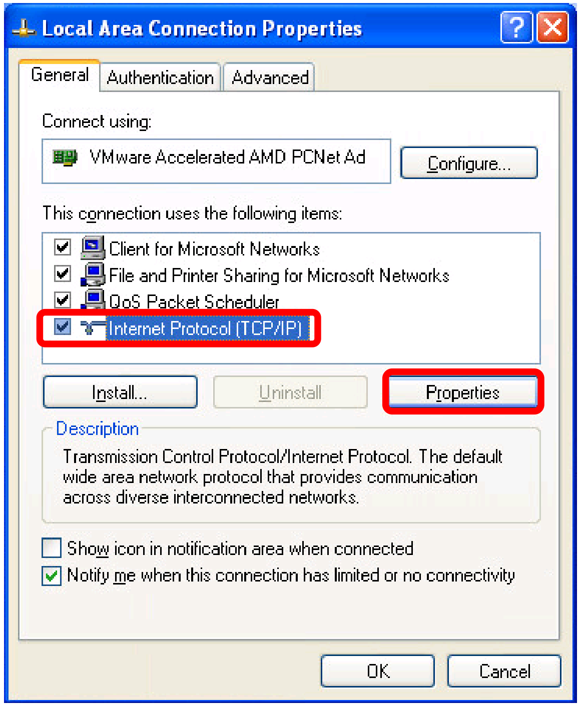
LAN

EH-pfSense-xx

EH-WinXP-xx


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections Go
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Acquiring network address, Fir...
VMware Accelerated AMD PCN...
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

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


Local Area Connection Properties
General Authentication Advanced
Configure...
Install... Uninstall Properties
OK Cancel

Connect using:

VMware Accelerated AMD PCNet Ad

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

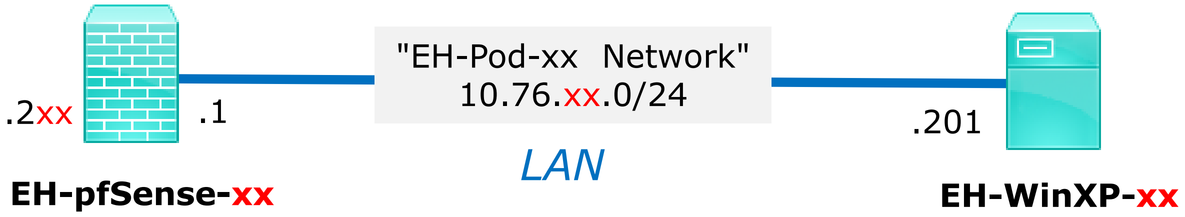
Description

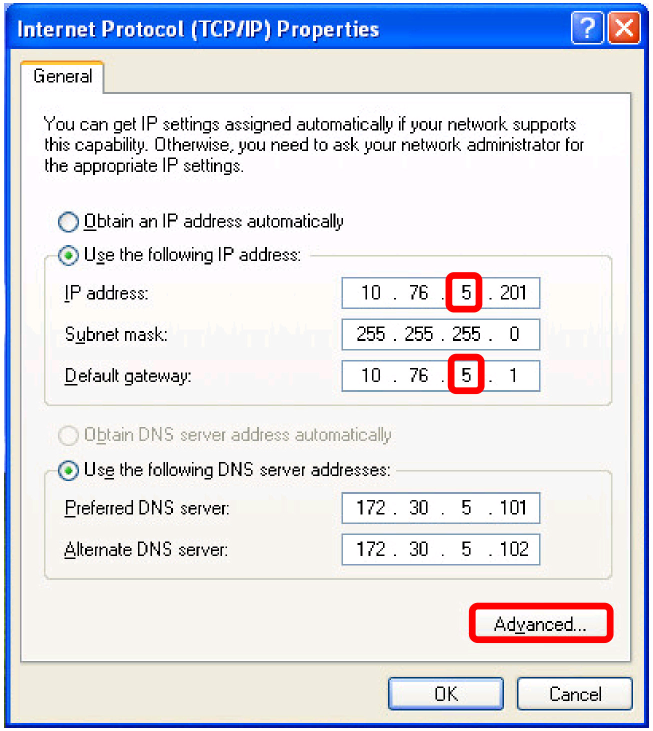
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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

Configuring the EH-WinXP VM in EH-Pod-xx





You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 76 . 5 . 201

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 76 . 5 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

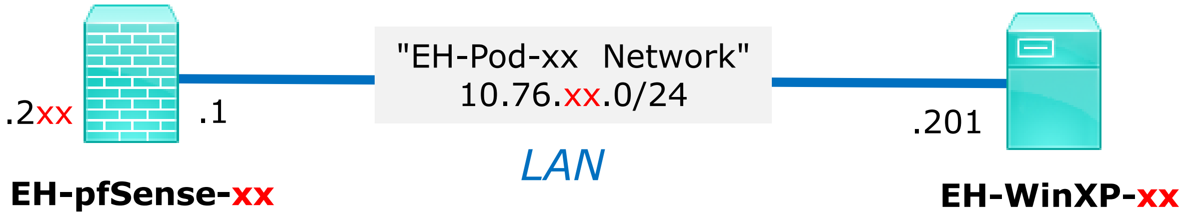
Preferred DNS server: 172 . 30 . 5 . 101

Alternate DNS server: 172 . 30 . 5 . 102

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

5) Next click the Advanced button.

Configuring the EH-WinXP VM in EH-Pod-xx

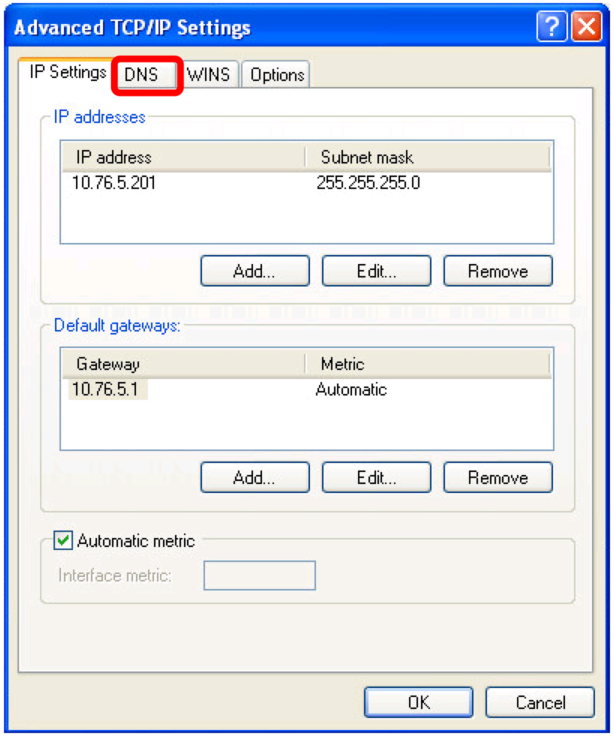


"EH-Pod-xx Network"
10.76.xx.0/24

LAN

.2xx .1 EH-pfSense-xx

.201 EH-WinXP-xx



Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

IP addresses

IP address	Subnet mask
10.76.5.201	255.255.255.0

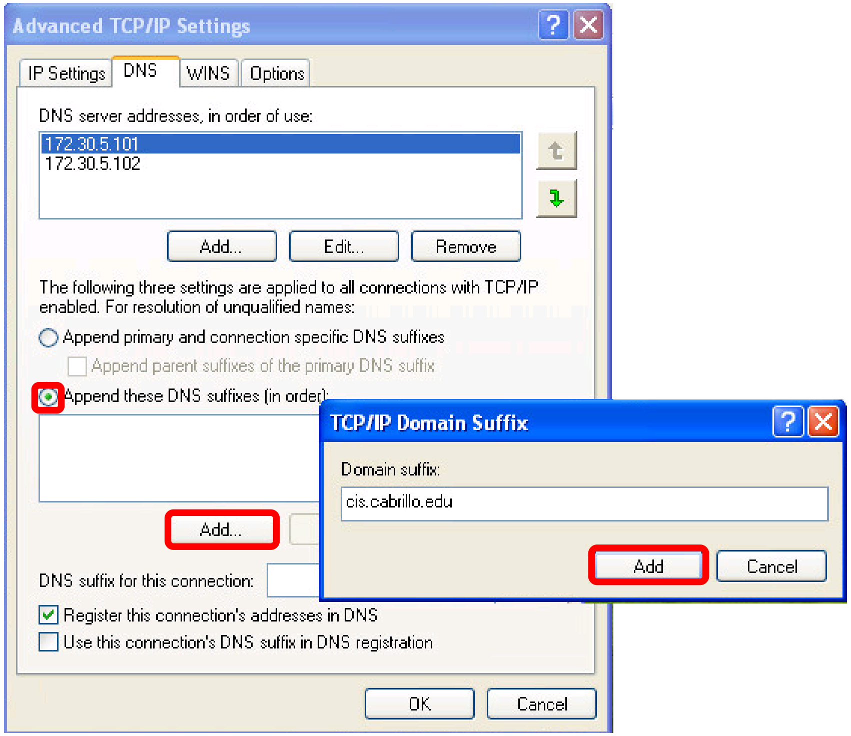
Default gateways:

Gateway	Metric
10.76.5.1	Automatic

☑ Automatic metric

Interface metric:

6) Click the DNS tab.



Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

DNS server addresses, in order of use:

172.30.5.101
172.30.5.102

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

○ Append primary and connection specific DNS suffixes

□ Append parent suffixes of the primary DNS suffix

● Append these DNS suffixes (in order):

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

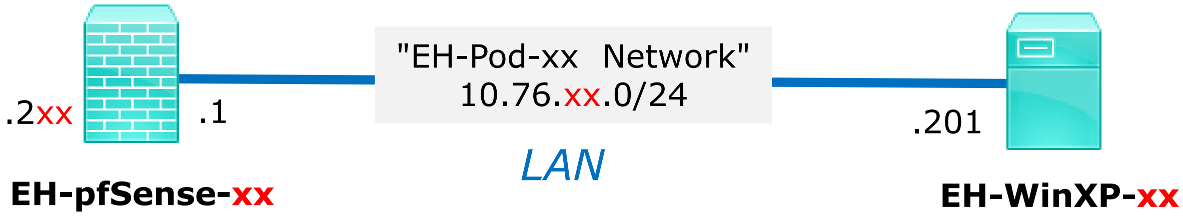
□ Use this connection's DNS suffix in DNS registration

TCP/IP Domain Suffix

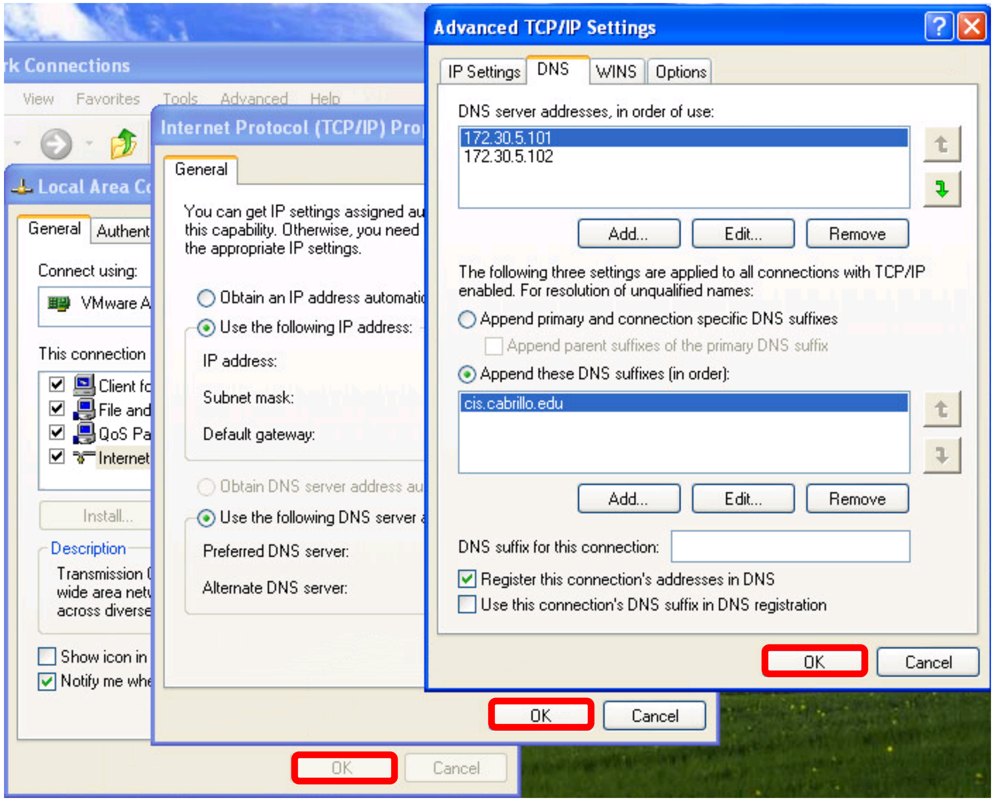
Domain suffix: cis.cabrillo.edu

7) Select "Append these DNS suffices (in order)", click the Add... button, type cis.cabrillo.edu as the Domain suffix then click Add button.

Configuring the EH-WinXP VM in EH-Pod-xx



8) Keep clicking OK buttons till you close all the TCP/IP and Connection dialog boxes.



Connect using:
VMware A

This connection
☑ Client fo
☑ File and
☑ QoS Pa
☑ Internet

Transmission (
wide area netw
across diverse

□ Show icon in
☑ Notify me whe

You can get IP settings assigned au
this capability. Otherwise, you need
the appropriate IP settings.

○ Obtain an IP address automatic
● Use the following IP address:
IP address:
Subnet mask:
Default gateway:

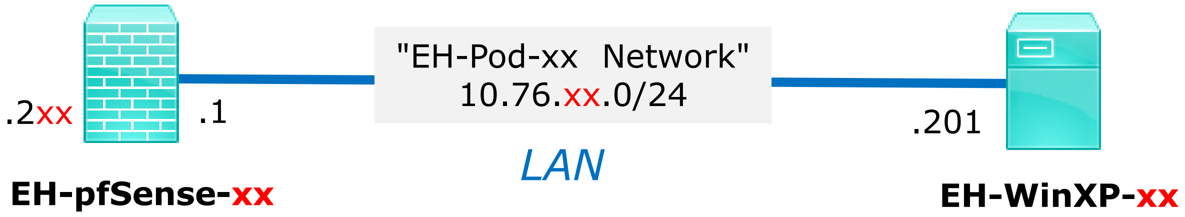
○ Obtain DNS server address au
● Use the following DNS server a
Preferred DNS server:
Alternate DNS server:

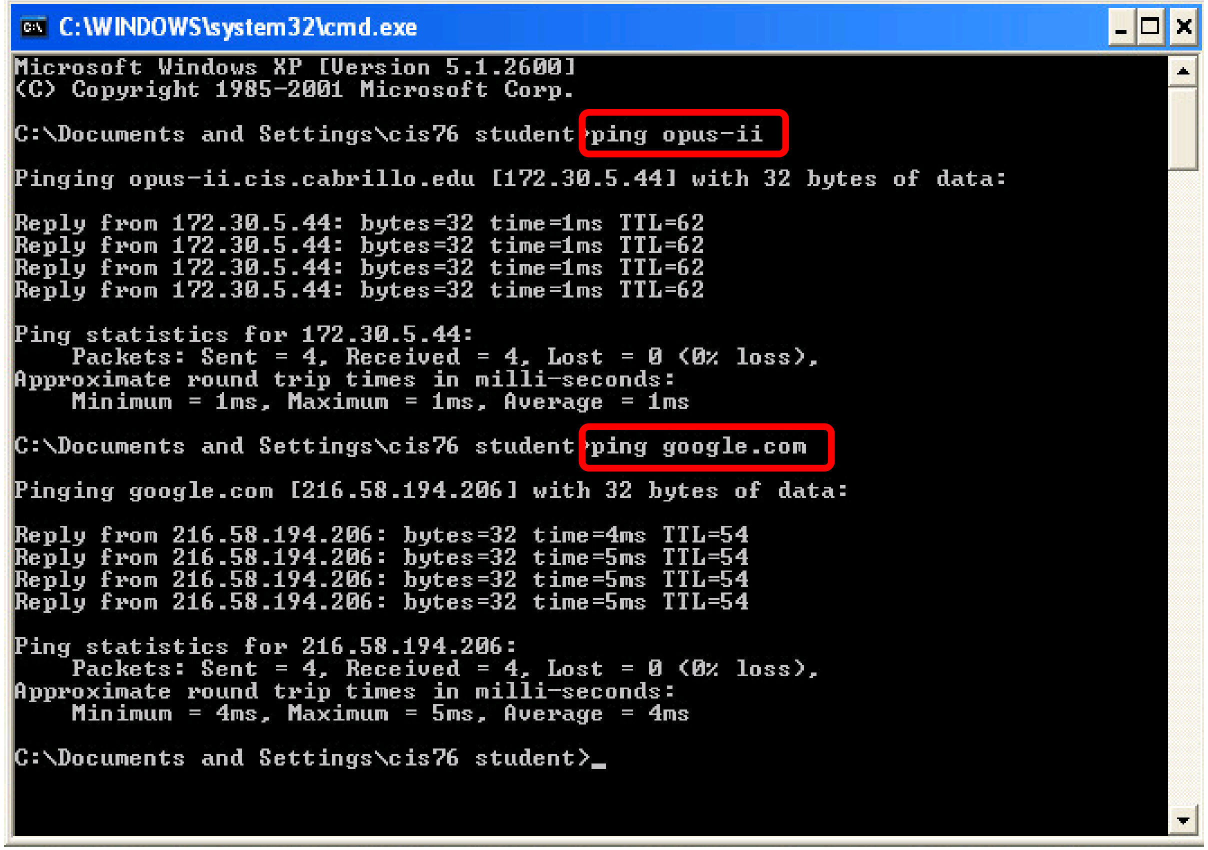
DNS server addresses, in order of use:
172.30.5.101
172.30.5.102

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:
○ Append primary and connection specific DNS suffixes
□ Append parent suffixes of the primary DNS suffix
● Append these DNS suffixes (in order):
cis.cabrillo.edu

DNS suffix for this connection:
☑ Register this connection's addresses in DNS
□ Use this connection's DNS suffix in DNS registration

Configuring the EH-WinXP VM in EH-Pod-xx



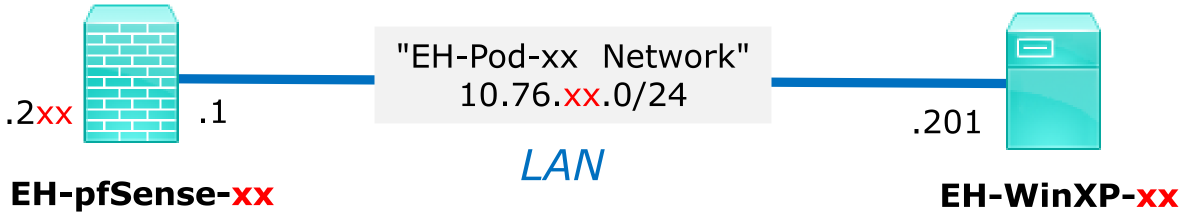


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>ping opus-ii

Pinging opus-ii.cis.cabrillo.edu [172.30.5.44] with 32 bytes of data:

Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62

Ping statistics for 172.30.5.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

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

Pinging google.com [216.58.194.206] with 32 bytes of data:

Reply from 216.58.194.206: bytes=32 time=4ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54

Ping statistics for 216.58.194.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

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

9) Run cmd.exe to bring up a command prompt. Ping opus-ii and google.com to verify your network settings.

Note, your pfSense VM must be configured and running or your pings will fail!

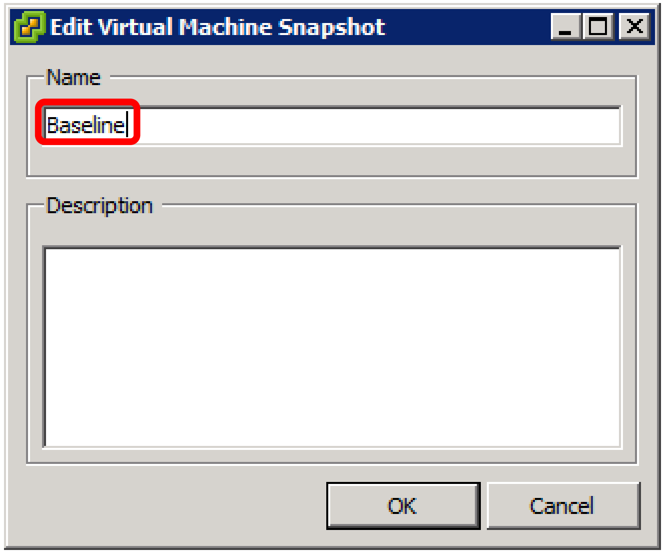
Configuring the EH-WinXP VM in EH-Pod-xx



Save your work

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

Now if you mess things up later can always start over again!



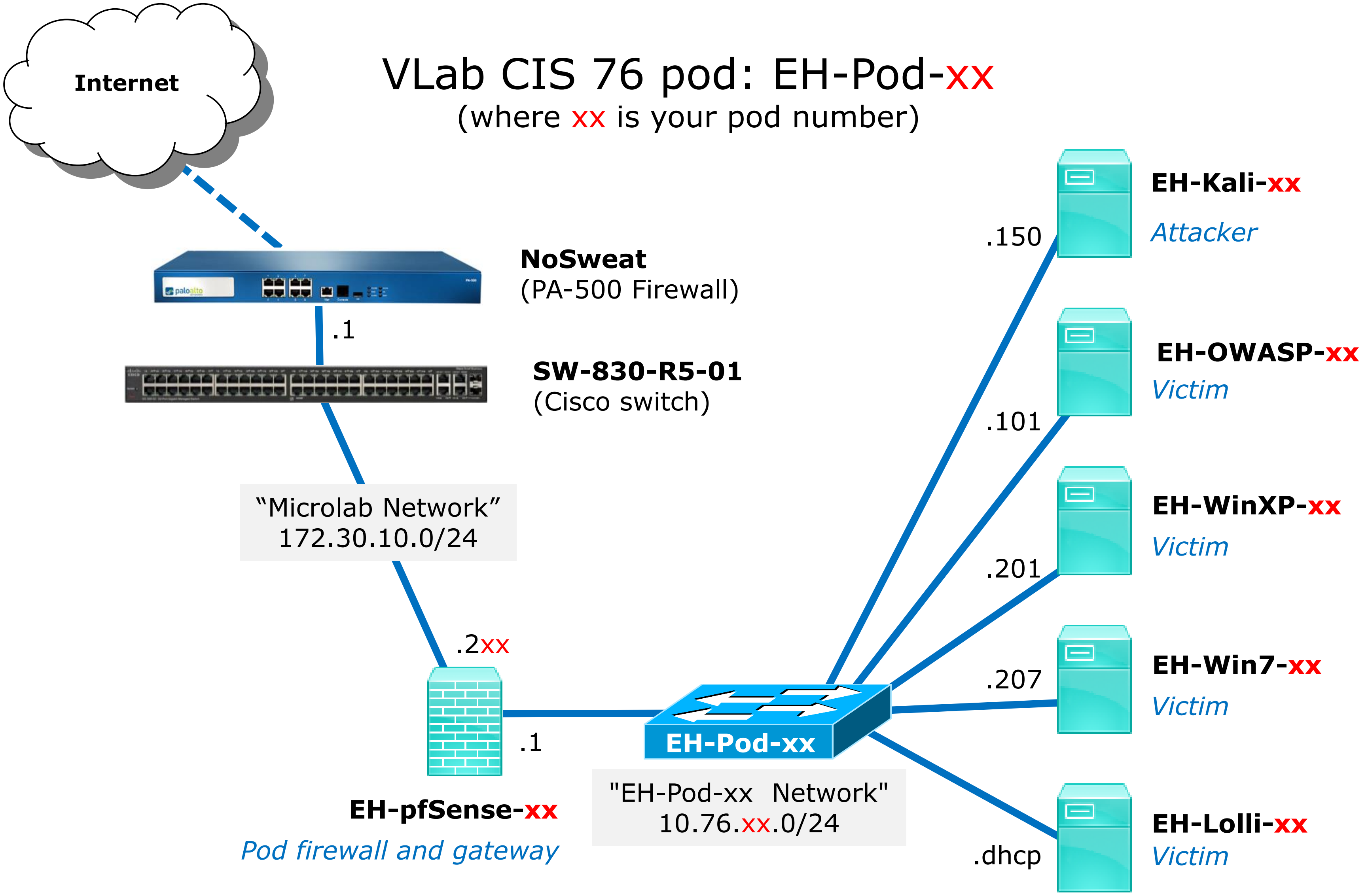
Name: Baseline

EH-Win7-xx
VM Config

CIS 76 - VLab Pod Setup

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



Internet

NoSweat
(PA-500 Firewall)

.1

SW-830-R5-01
(Cisco switch)

"Microlab Network"
172.30.10.0/24

.2xx

.1

EH-pfSense-xx
Pod firewall and gateway

EH-Pod-xx

"EH-Pod-xx Network"
10.76.xx.0/24

.150
EH-Kali-xx
Attacker

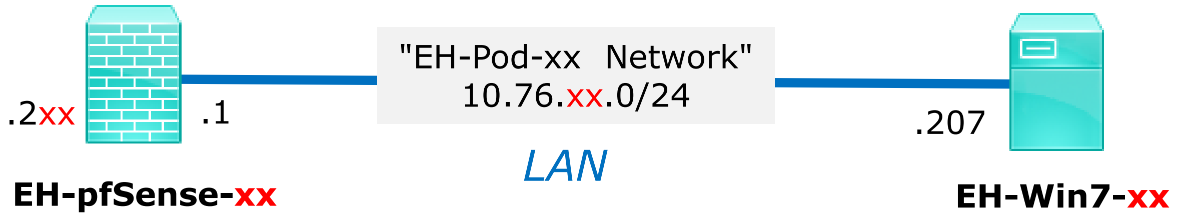
.101
EH-OWASP-xx
Victim

.201
EH-WinXP-xx
Victim

.207
EH-Win7-xx
Victim

.dhcp
EH-Lolli-xx
Victim

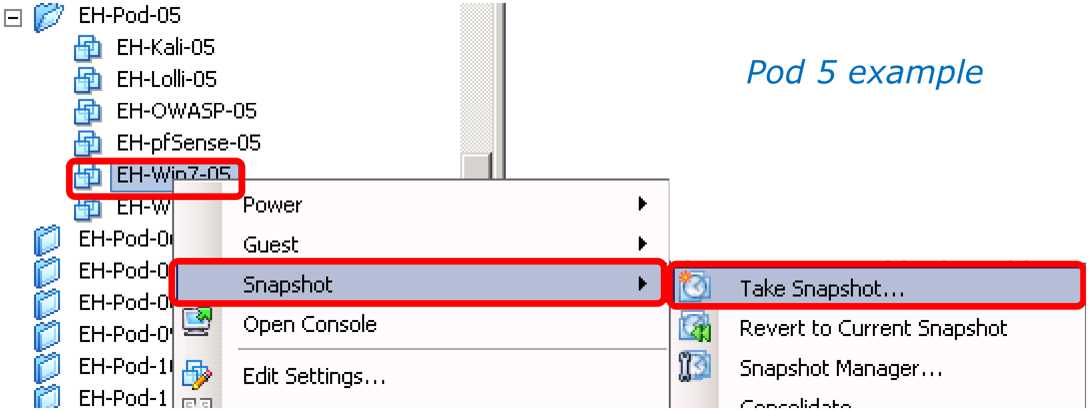
Configuring the EH-Win7 VM in EH-Pod-xx



xx is the pod number assigned to you.

Win7 VM	Pod xx settings
VM Network Adapter 1	EH-Pod-xx Net
Computer Name	EH-Win7-xx
IPv4 address	10.76.xx.207
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.xx.1
Network location	Work network
Preferred DNS server	172.30.5.101
Alternate DNS server	172.30.5.102
Domain suffix	cis.cabrillo.edu

Configuring the EH-Win7 VM in EH-Pod-05

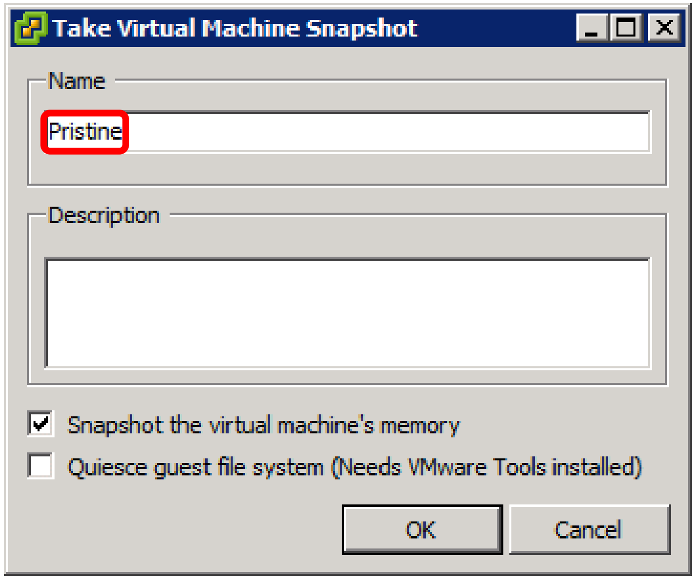


Pod 5 example

IMPORTANT, back up your VM!

1) Make a backup snapshot of your Win7 VM named "**Pristine**".

Now if you mess things up you can always start over again!



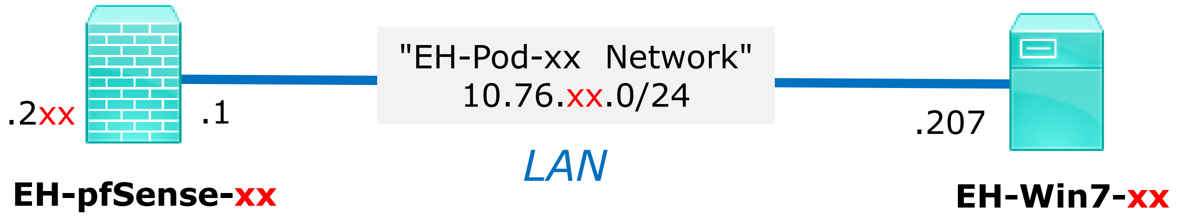
Name: Pristine

Description:

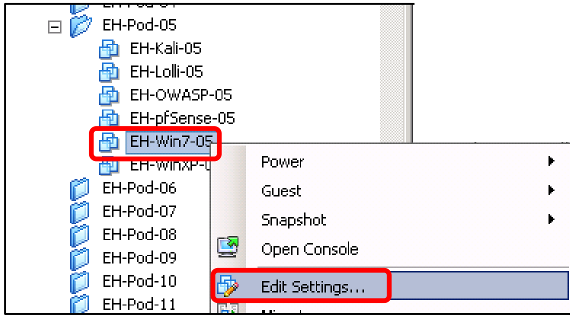
☑ Snapshot the virtual machine's memory

□ Quiesce guest file system (Needs VMware Tools installed)

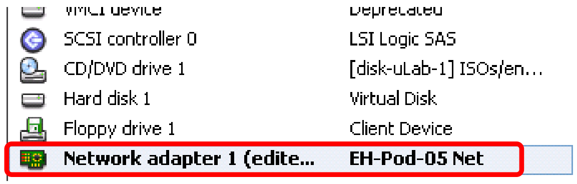
Configuring the EH-Win7 VM in EH-Pod-xx



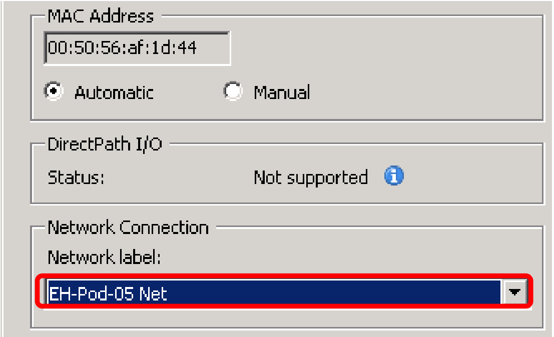
.2xx
.1
"EH-Pod-xx Network"
10.76.xx.0/24
LAN
.207
EH-pfSense-xx
EH-Win7-xx



- EH-Pod-05
  - EH-Kali-05
  - EH-Lolli-05
  - EH-OWASP-05
  - EH-pfSense-05
  - EH-Win7-05
  - EH-WinXP-0
- EH-Pod-06
- EH-Pod-07
- EH-Pod-08
- EH-Pod-09
- EH-Pod-10
- EH-Pod-11



VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
CD/DVD drive 1	[disk-uLab-1] ISOs/en...
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1 (edite...	**EH-Pod-05 Net**



MAC Address
00:50:56:af:1d:44
● Automatic ○ Manual

DirectPath I/O
Status: Not supported

Network Connection
Network label:
EH-Pod-05 Net

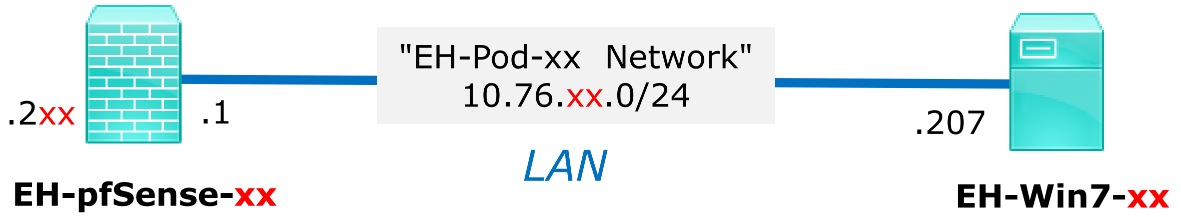
Pod 5 example

Network Cabling

1) Edit the settings of your Win7 VM.

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

Configuring the EH-Win7 VM in EH-Pod-xx

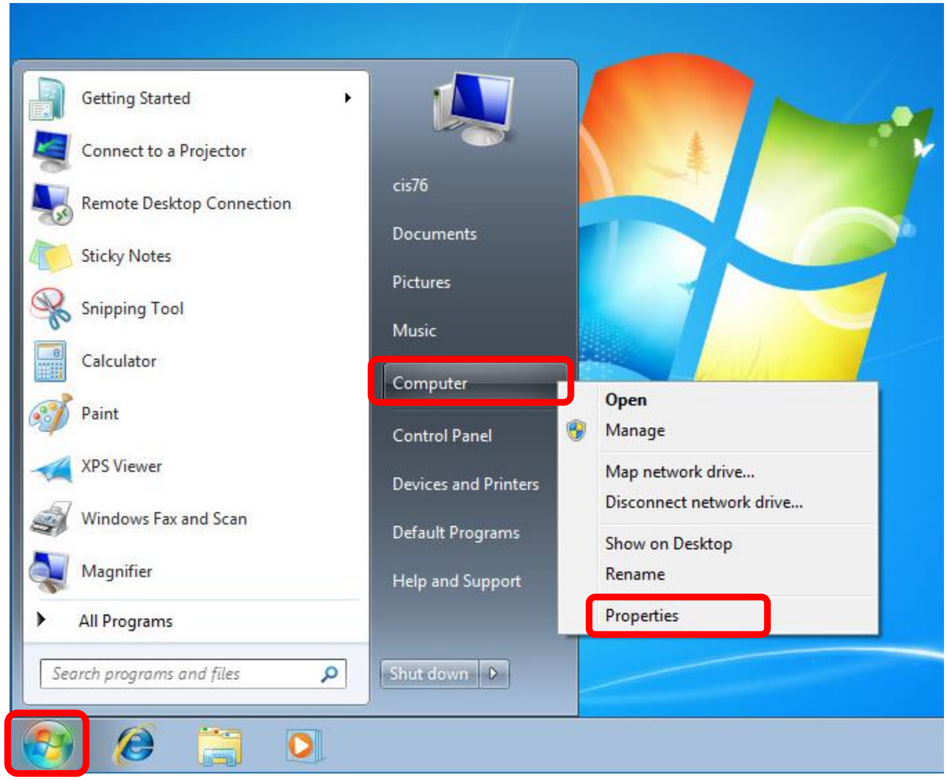


Computer Name Configuration

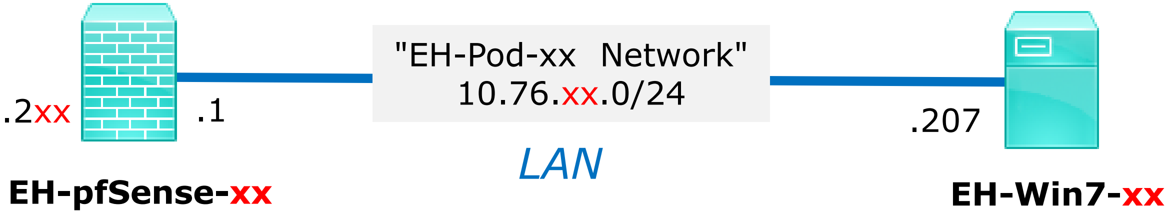
1) Power up the VM and open a console.

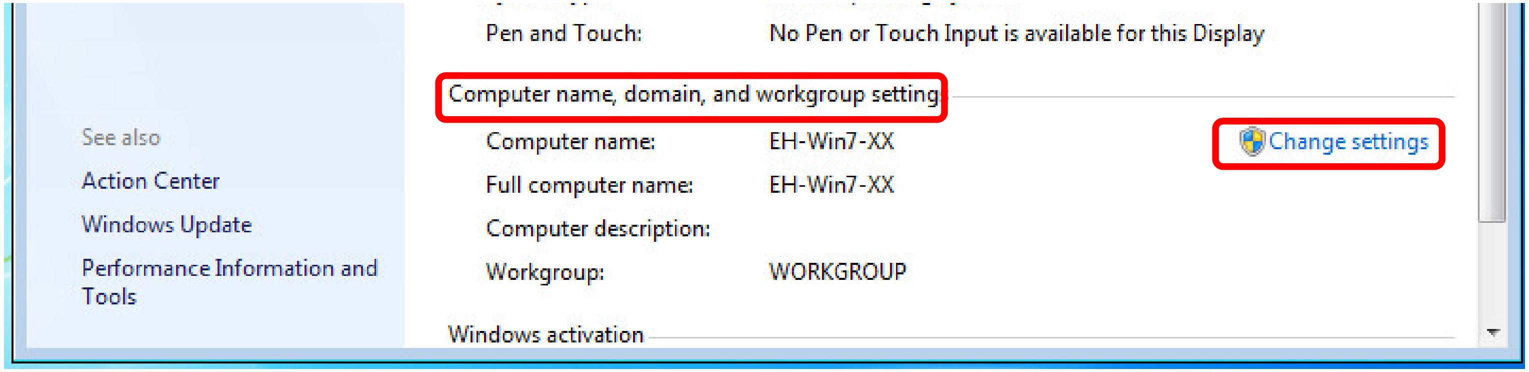
2) After Setup finishes and restarts, login as the cis76 user.

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



Configuring the EH-Win7 VM in EH-Pod-xx





Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: EH-Win7-XX

Full computer name: EH-Win7-XX

Computer description:

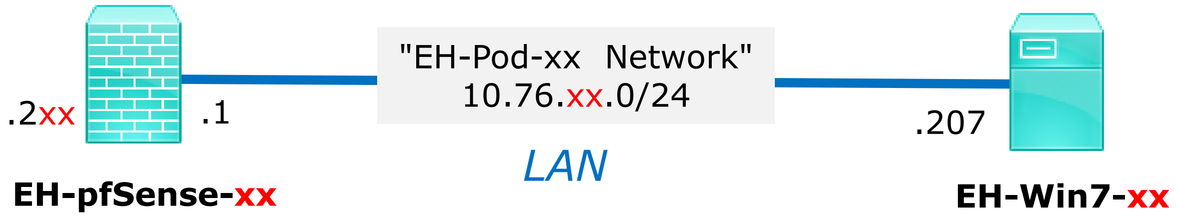
Workgroup: WORKGROUP

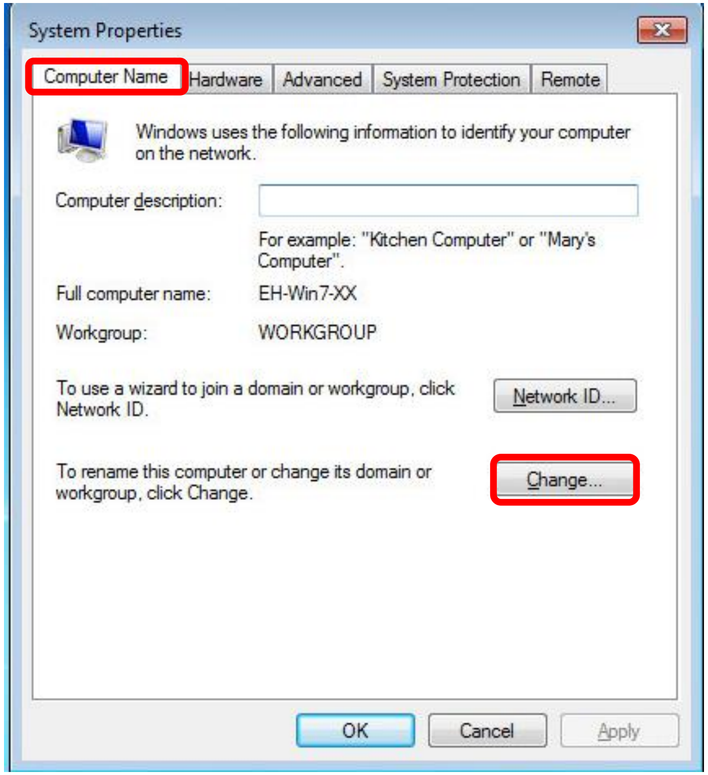
Windows activation

4) Look for Computer name, domain and workgroup settings.

5) Click Change settings

Configuring the EH-Win7 VM in EH-Pod-xx





System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: EH-Win7-XX

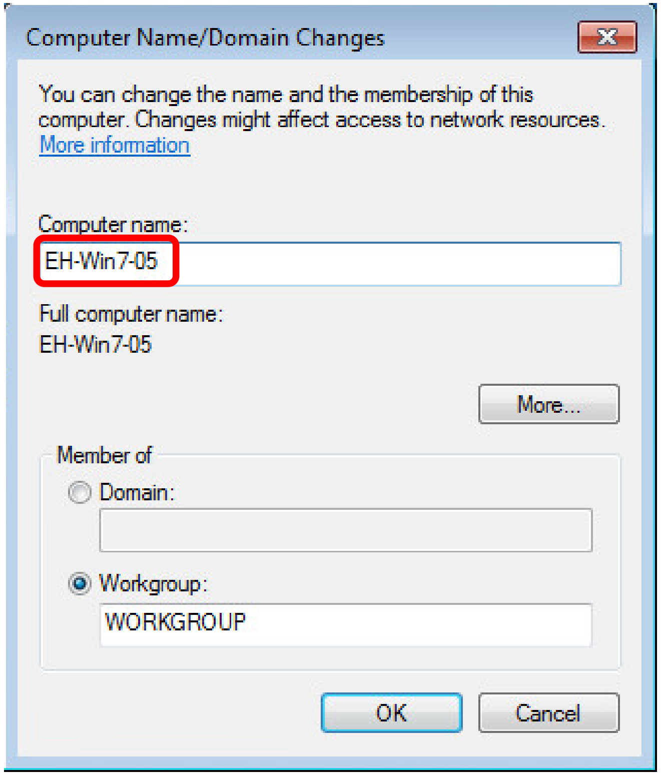
Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID. [Network ID...]

To rename this computer or change its domain or workgroup, click Change. [Change...]

[OK] [Cancel] [Apply]

6) Click the Computer Name tab then click Change button.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: EH-Win7-05

Full computer name:
EH-Win7-05

[More...]

Member of

○ Domain:

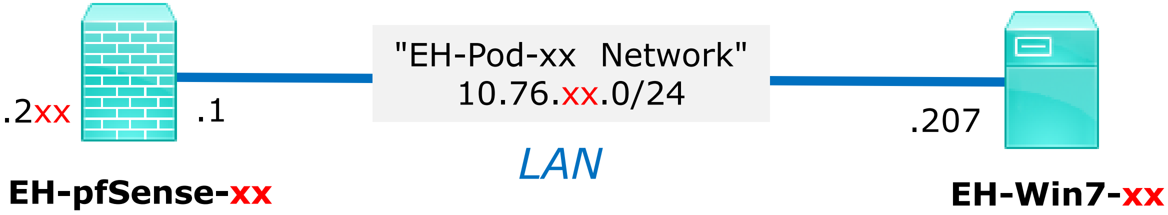
● Workgroup: WORKGROUP

[OK] [Cancel]

Pod 5 example

7) Update the Computer name with your two digit pod number. Click OK twice, then Close, then restart the VM.

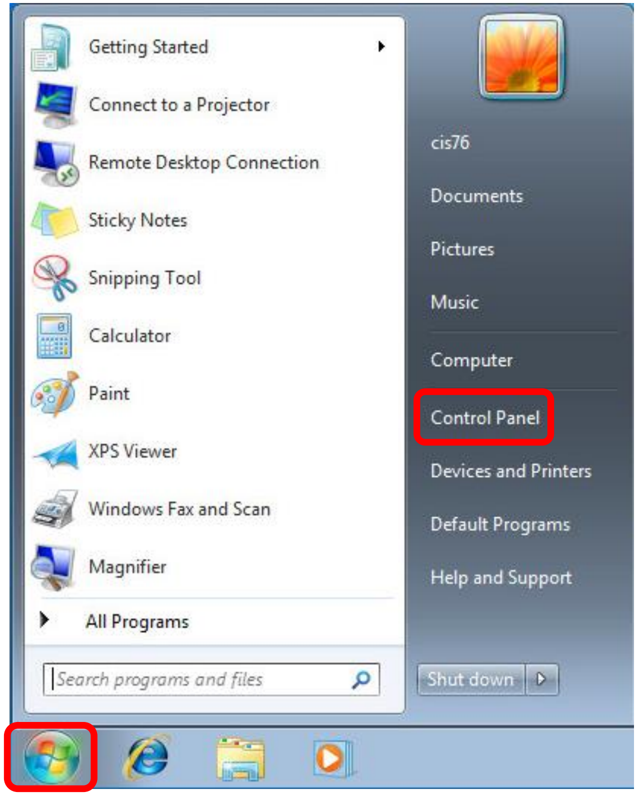
Configuring the EH-Win7 VM in EH-Pod-xx



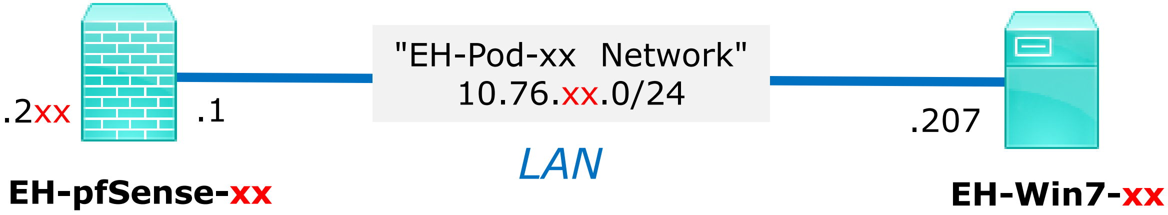
Network Configuration

1) Login back in as the cis76 user.

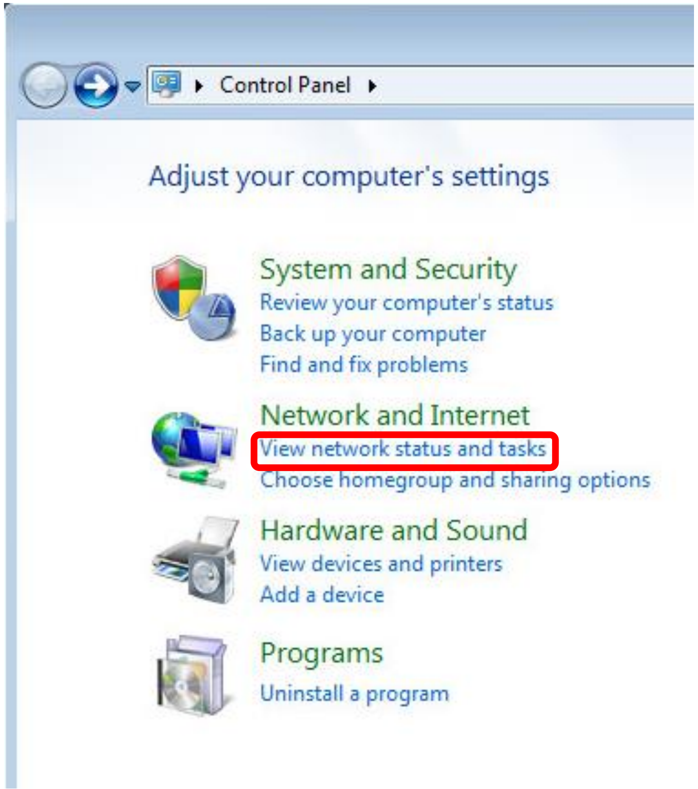
2) Click Start, then click on Control Panel.



Configuring the EH-Win7 VM in EH-Pod-xx



3) Click View network status and tasks.



Adjust your computer's settings

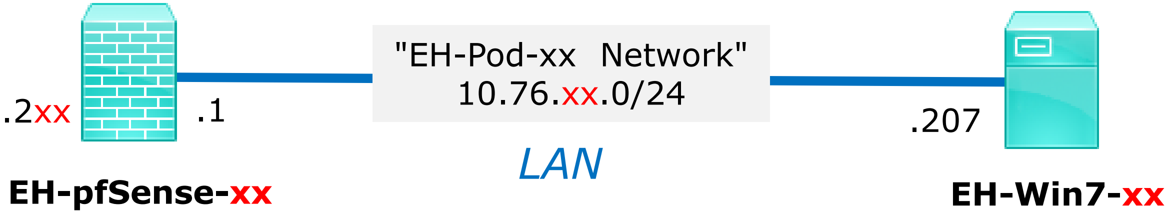
System and Security
Review your computer's status
Back up your computer
Find and fix problems

Network and Internet
View network status and tasks
Choose homegroup and sharing options

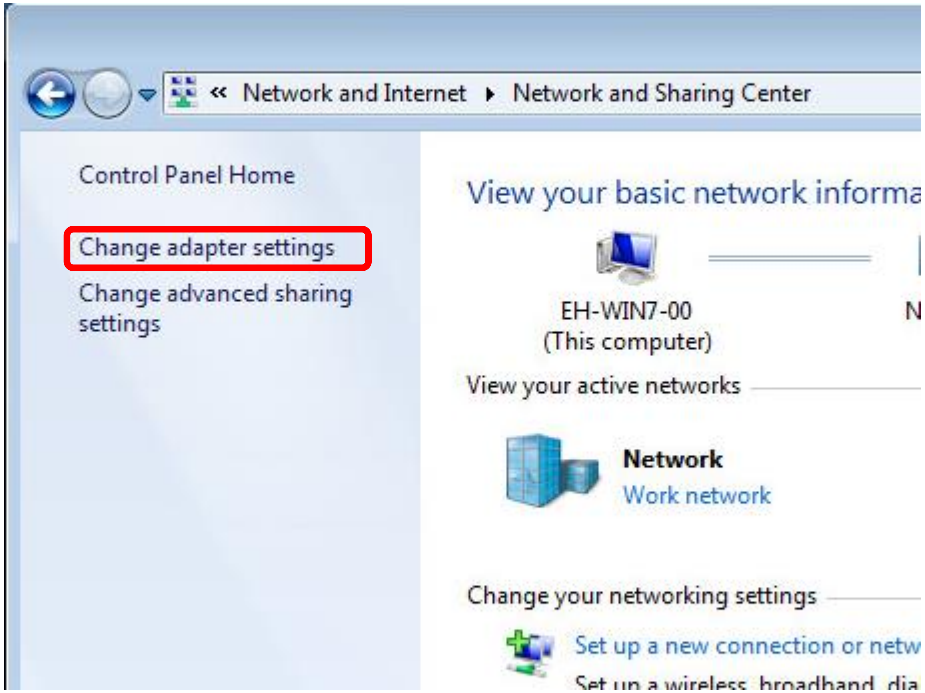
Hardware and Sound
View devices and printers
Add a device

Programs
Uninstall a program

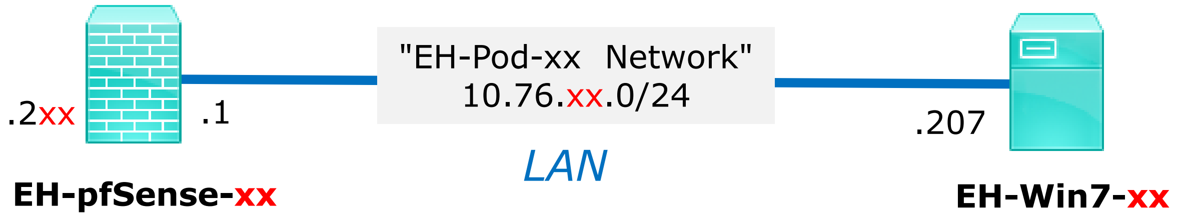
Configuring the EH-Win7 VM in EH-Pod-xx

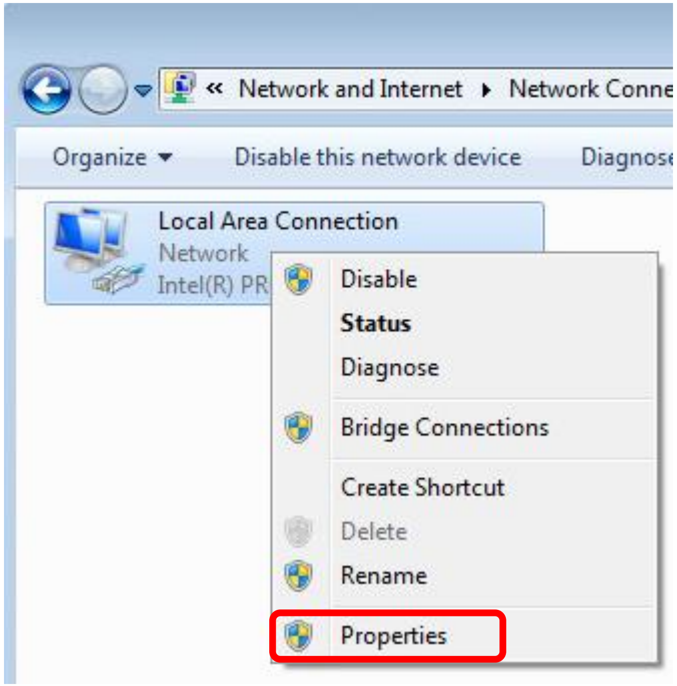


4) Click Change adapter settings

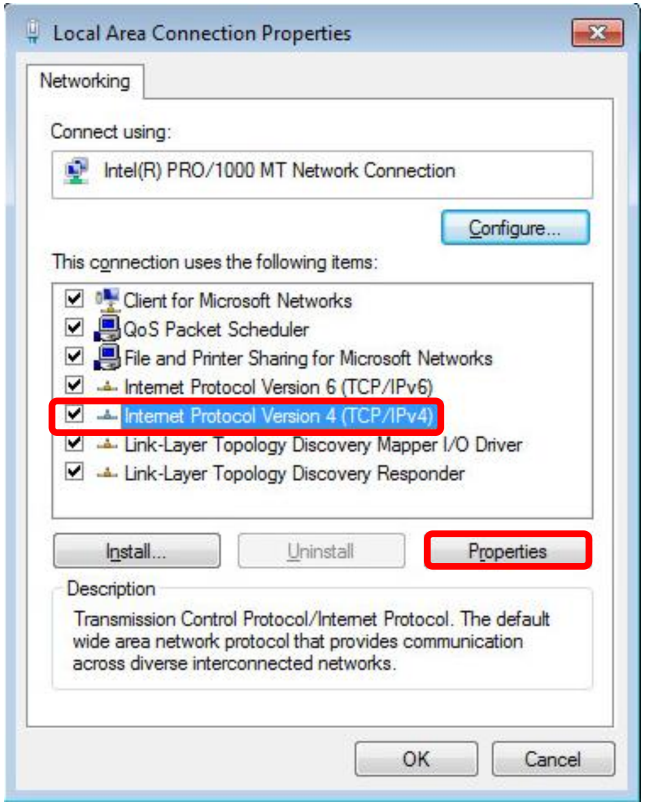

« Network and Internet ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network informa
EH-WIN7-00
(This computer)
N
View your active networks
Network
Work network
Change your networking settings
Set up a new connection or netw
Set up a wireless, broadband, dia

Configuring the EH-Win7 VM in EH-Pod-xx





5) Right-click on the Local Area Connection and select Properties.



Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

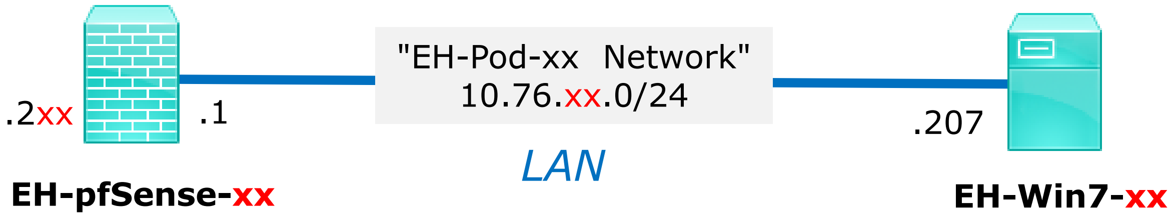
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6) Select Internet Protocol Version 4 (TCP/IP) and click on Properties.

Configuring the EH-Win7 VM in EH-Pod-xx



.2xx .1

"EH-Pod-xx Network"
10.76.xx.0/24

.207

LAN

EH-pfSense-xx

EH-Win7-xx

Set a static (non-DHCP) address on your EH-Win7 VM

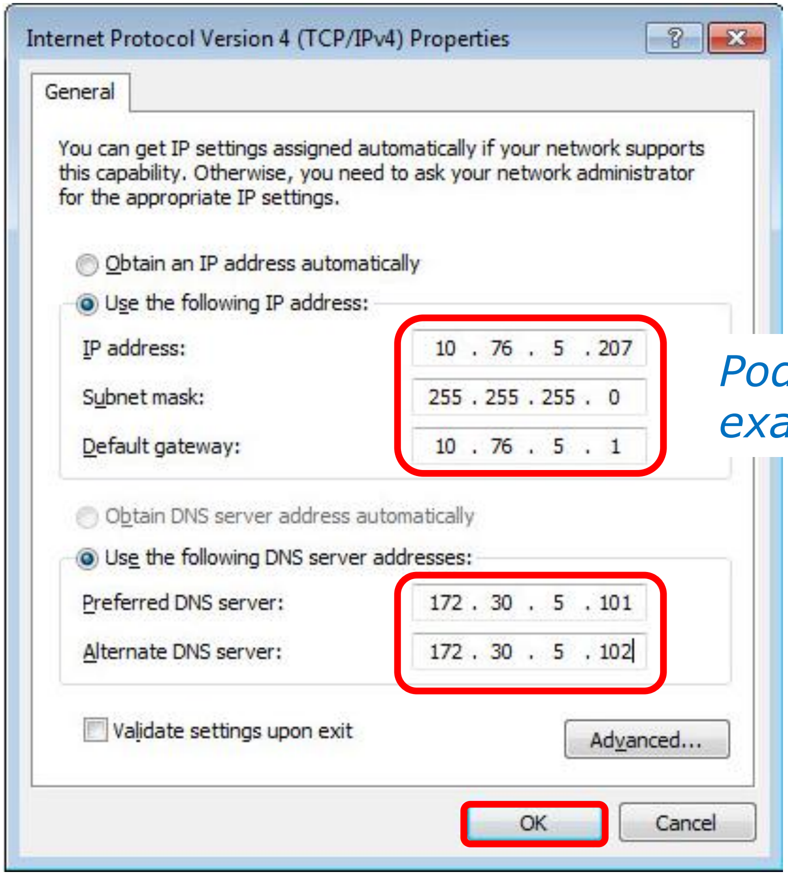
7) Configure the IPv4 address to **10.76.xx.207** (where xx is your pod number).

8) Set **255.255.255.0** as the Subnet Mask.

9) Configure the Default Gateway to **10.76.xx.1** (where xx is your pod number)

10) Add the two CIS name servers **172.30.5.101** and **172.30.5.102**

11) Click OK, then Close.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 76 . 5 . 207

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 76 . 5 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

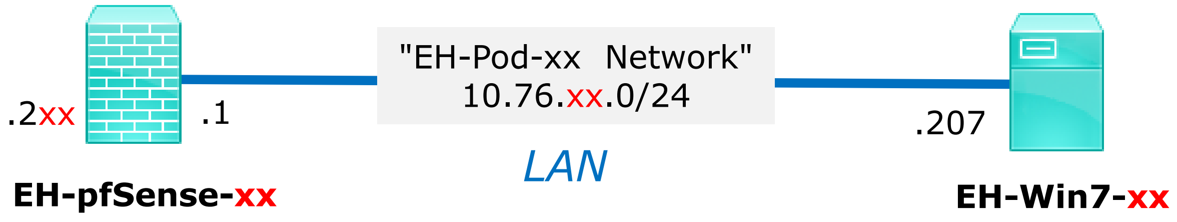
Preferred DNS server: 172 . 30 . 5 . 101

Alternate DNS server: 172 . 30 . 5 . 102

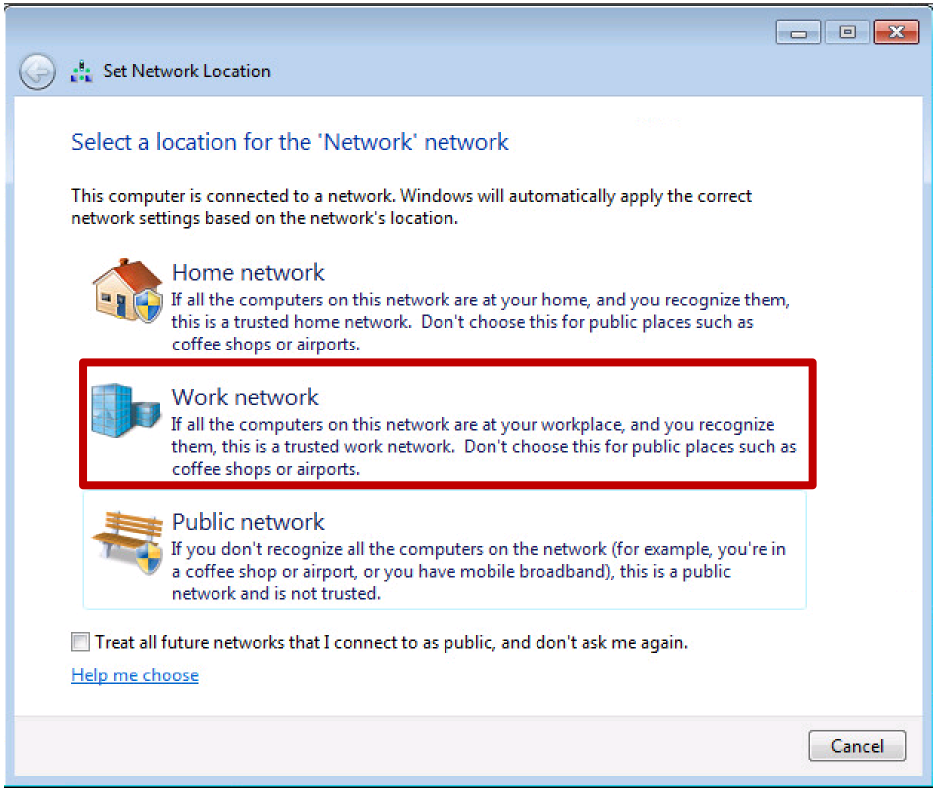
□ Validate settings upon exit

Pod 5 example

Configuring the EH-Win7 VM in EH-Pod-xx



If prompted for a network location select "Work network"


Set Network Location

Select a location for the 'Network' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

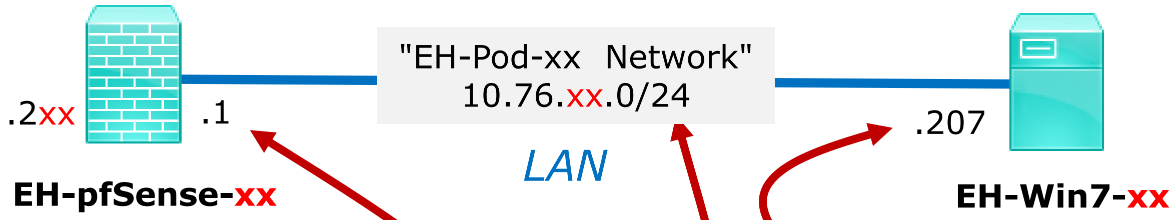
Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

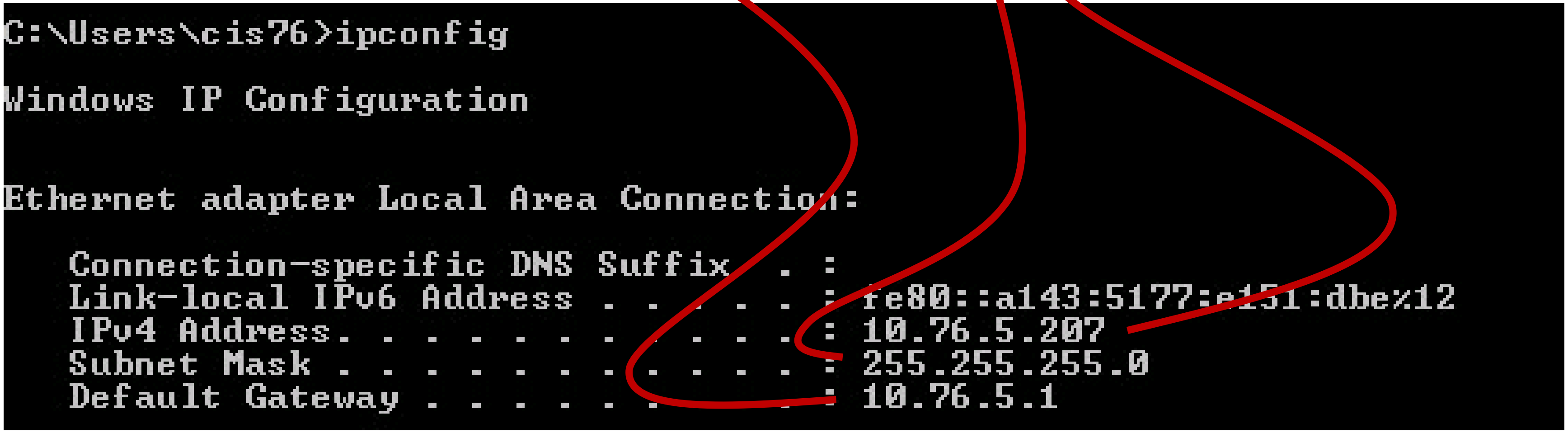
Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

☐ Treat all future networks that I connect to as public, and don't ask me again.

Configuring the EH-Win7 VM in EH-Pod-xx



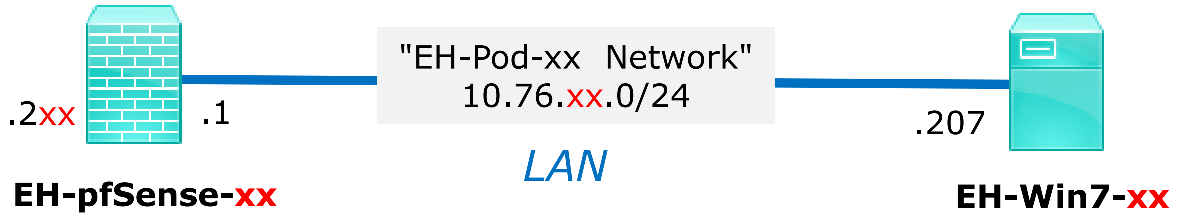


```
C:\Users\cis76>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a143:5177:e151:dbe%12
   IPv4 Address. . . . . . . . . . . : 10.76.5.207
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.76.5.1
```

Pod 5 example

12) Using cmd.exe, run the **ipconfig** command and check your IP settings.

Configuring the EH-Win7 VM in EH-Pod-xx



.2xx

.1

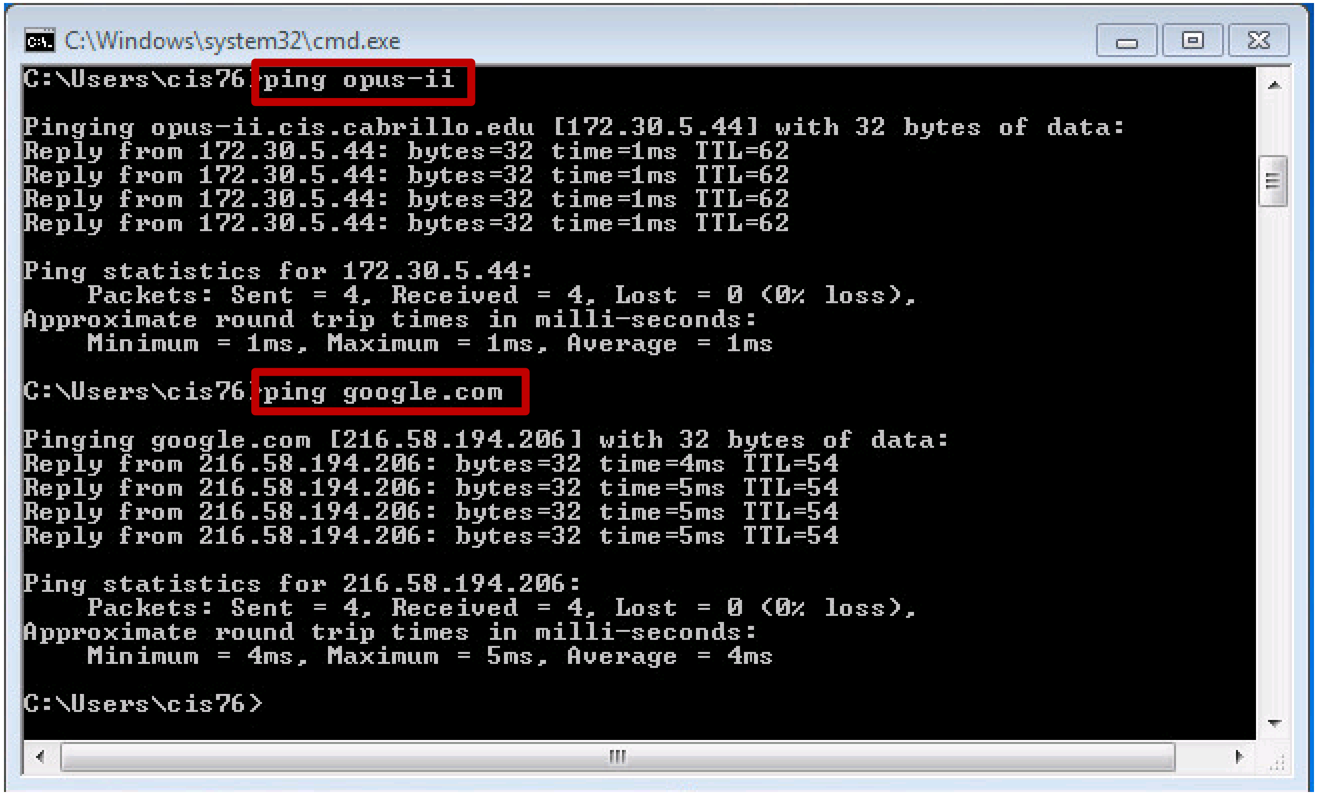
"EH-Pod-xx Network"
10.76.xx.0/24

LAN

.207

EH-pfSense-xx

EH-Win7-xx



```
C:\Users\cis76>ping opus-ii

Pinging opus-ii.cis.cabrillo.edu [172.30.5.44] with 32 bytes of data:
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62
Reply from 172.30.5.44: bytes=32 time=1ms TTL=62

Ping statistics for 172.30.5.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\cis76>ping google.com

Pinging google.com [216.58.194.206] with 32 bytes of data:
Reply from 216.58.194.206: bytes=32 time=4ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54
Reply from 216.58.194.206: bytes=32 time=5ms TTL=54

Ping statistics for 216.58.194.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\cis76>
```

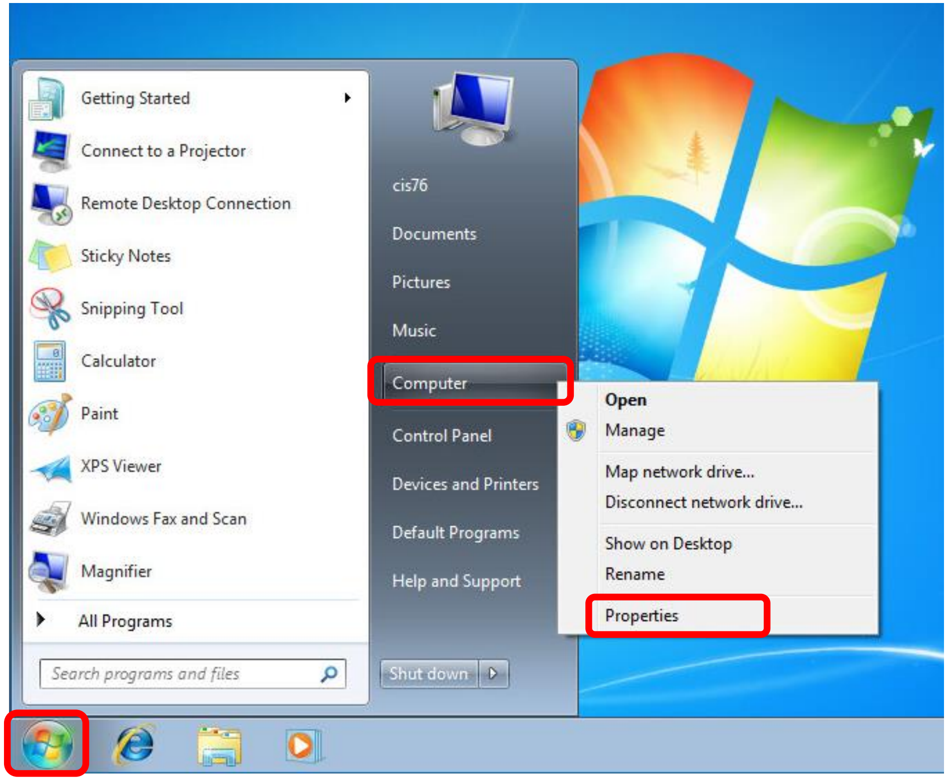
13) Using cmd.exe, verify you can ping opus-ii and google.com.

Configuring the EH-Win7 VM in EH-Pod-xx

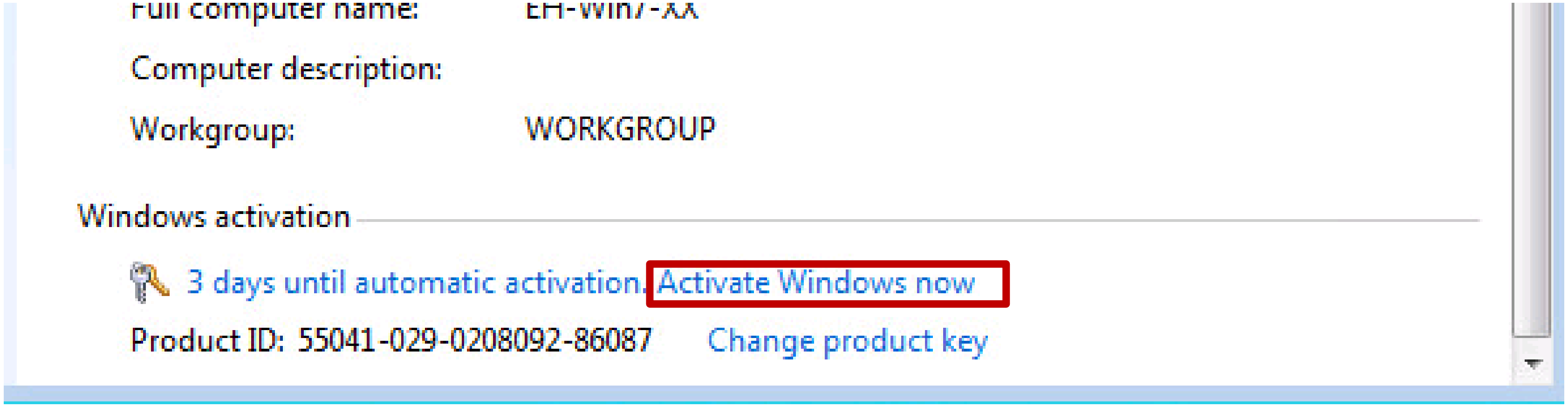
Activation

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

Don't try and activate Windows till your Internet connection is working.



Configuring the EH-Win7 VM in EH-Pod-xx



Full computer name: EH-Win7-XX

Computer description:

Workgroup: WORKGROUP

Windows activation

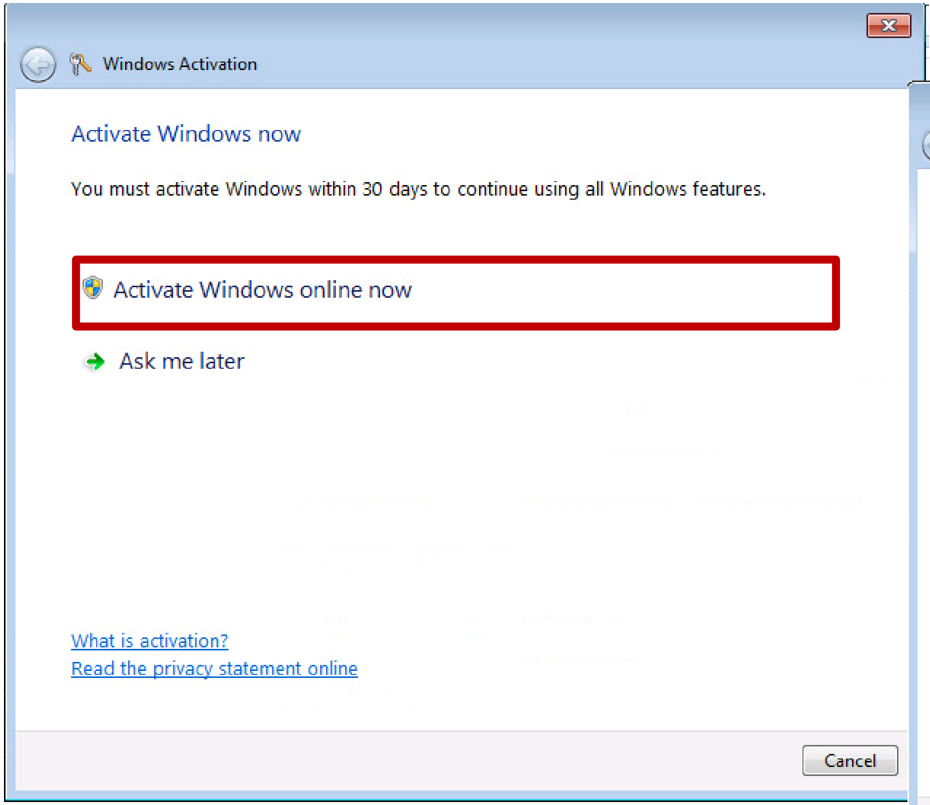
3 days until automatic activation. Activate Windows now

Product ID: 55041-029-0208092-86087 Change product key

2) Scroll down and look for Windows activation section.

3) Click "Activate Windows now"

CIS 76 - VLab Pod Setup

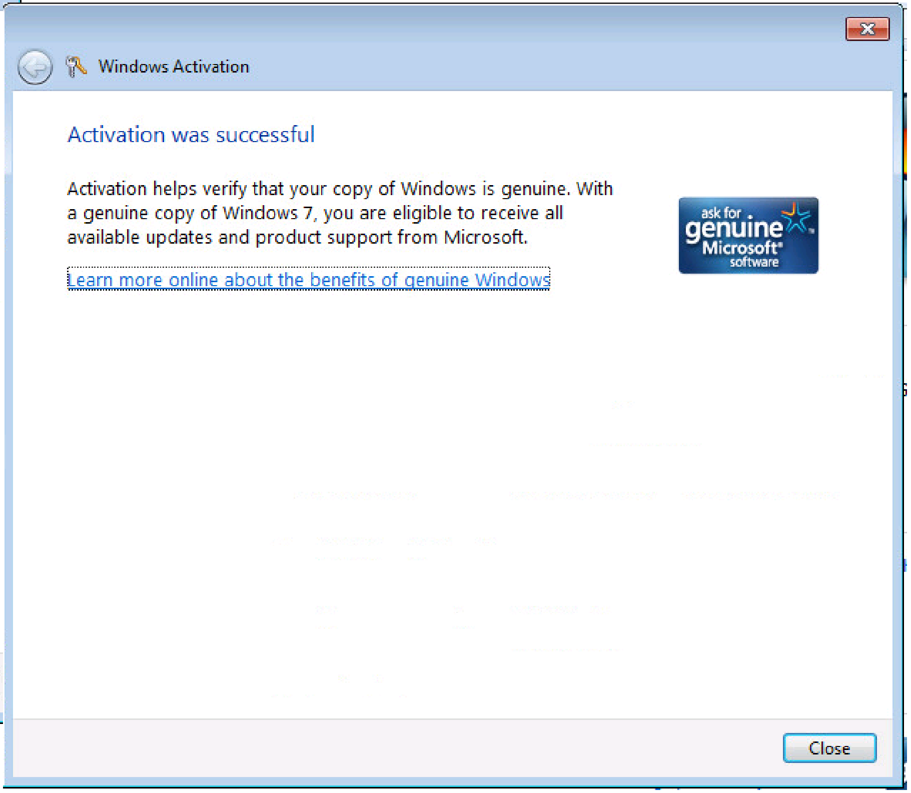


Windows Activation

Activate Windows now

You must activate Windows within 30 days to continue using all Windows features.

Activate Windows online now
Ask me later
What is activation?
Read the privacy statement online
Cancel



Windows Activation

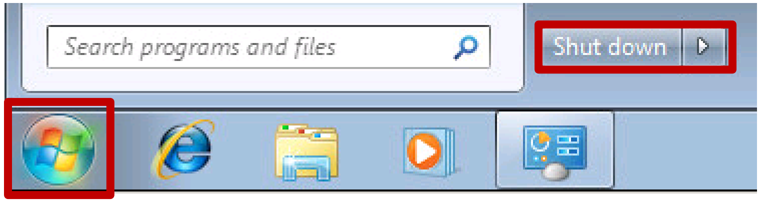
Activation was successful

Activation helps verify that your copy of Windows is genuine. With a genuine copy of Windows 7, you are eligible to receive all available updates and product support from Microsoft.

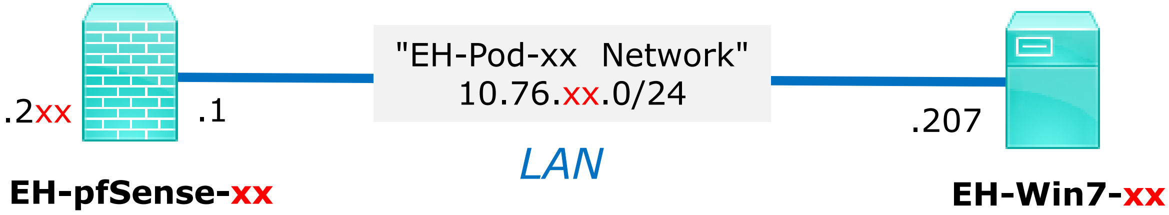
Learn more online about the benefits of genuine Windows
ask for genuine Microsoft software
Close

4) Click "Activate Windows online now"

5) After a successful activation shutdown the VM (Start > Shutdown button)



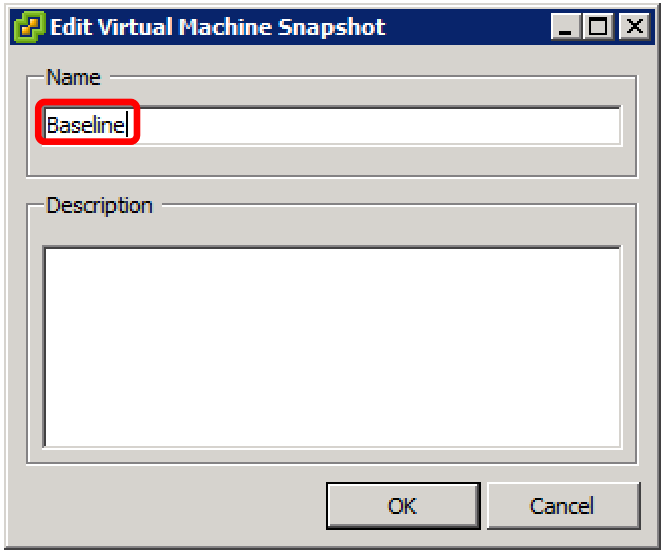
Configuring the EH-Win7 VM in EH-Pod-xx



Save your work

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

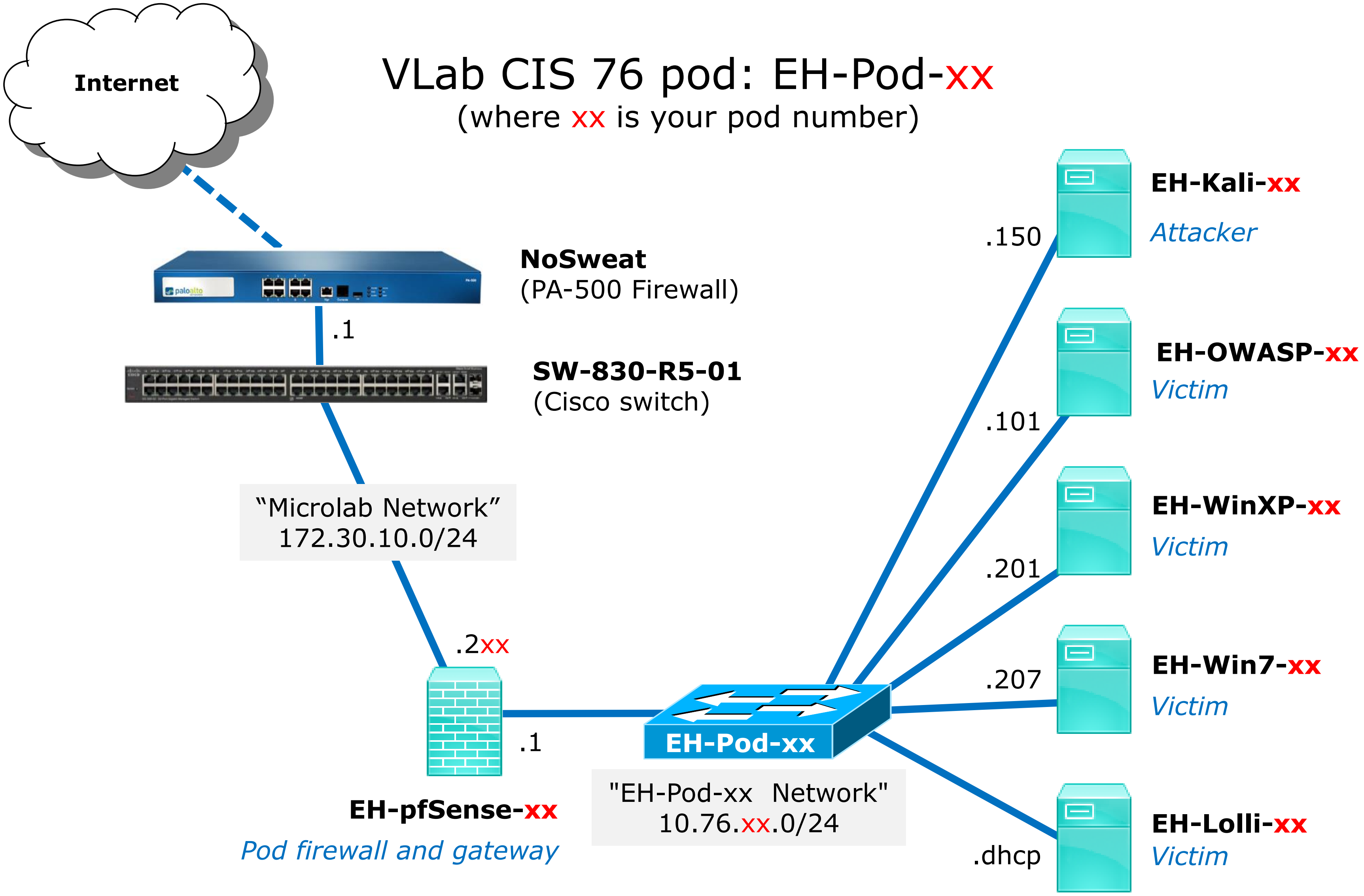
Now if you mess things up later can always start over again!



Name: Baseline

EH-OWASP-xx VM Config

CIS 76 - VLab Pod Setup



VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)

Internet

NoSweat
(PA-500 Firewall)

.1

SW-830-R5-01
(Cisco switch)

"Microlab Network"
172.30.10.0/24

.2xx

.1

EH-pfSense-xx
Pod firewall and gateway

EH-Pod-xx

"EH-Pod-xx Network"
10.76.xx.0/24

.150 **EH-Kali-xx**
Attacker

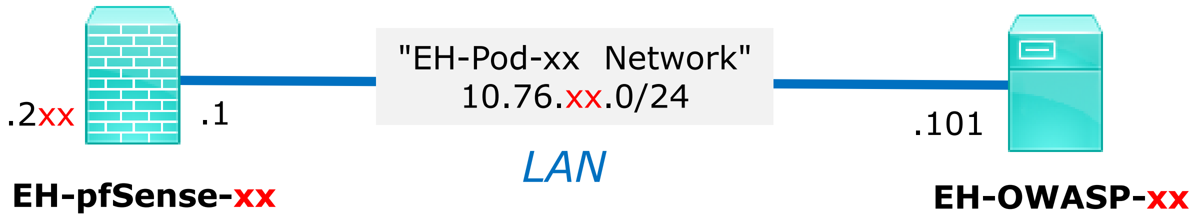
.101 **EH-OWASP-xx**
Victim

.201 **EH-WinXP-xx**
Victim

.207 **EH-Win7-xx**
Victim

.dhcp **EH-Lolli-xx**
Victim

Configuring the EH-OWASP VM in EH-Pod-xx

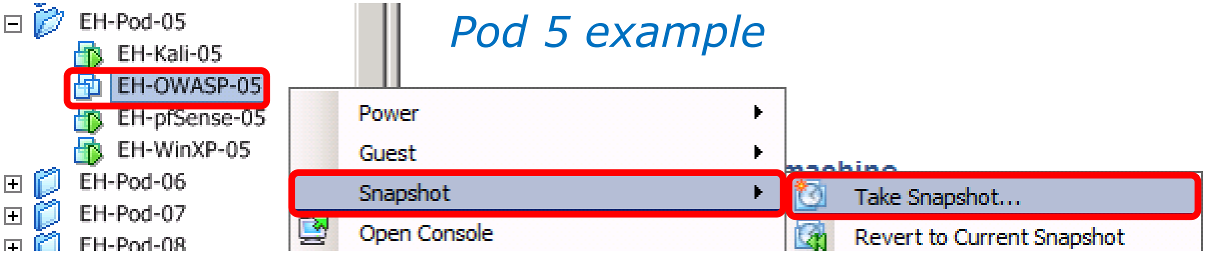


This example shows pod 5.

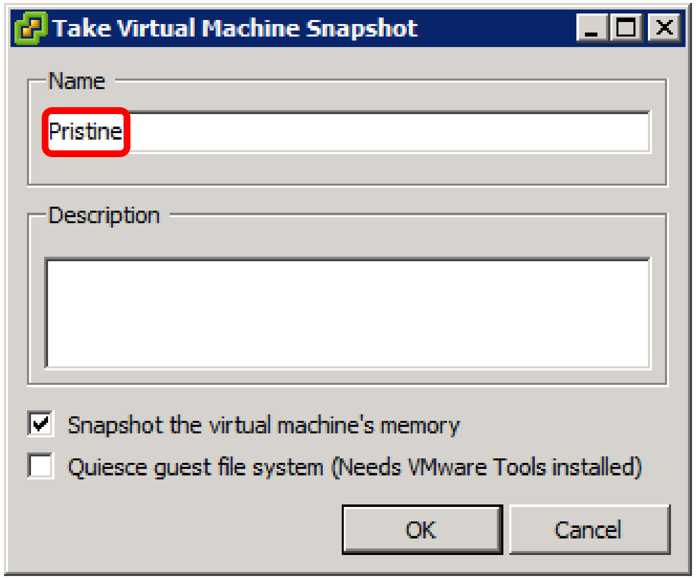
Each student should only use the pod assigned to them.

OWASP VM	Pod xx settings
VM Network Adapter 1	EH-Pod-xx Net
IPv4 address	10.76.x.101
IPv4 netmask	255.255.255.0
IPv4 gateway	10.76.x.1
Domain search string	cis.cabrillo.edu
Name servers	172.30.5.101 172.30.5.102

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



Pod 5 example


Take Virtual Machine Snapshot

Name

Pristine

Description

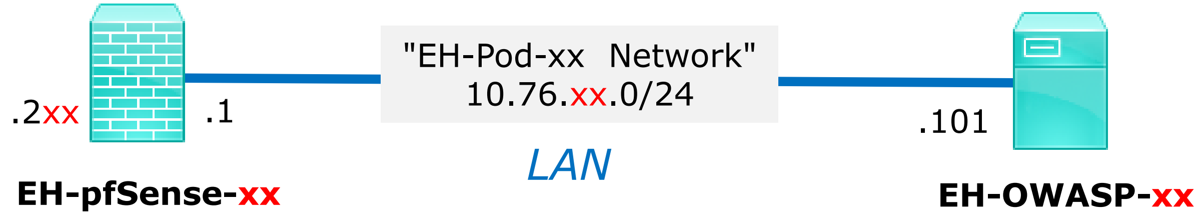
☑ Snapshot the virtual machine's memory

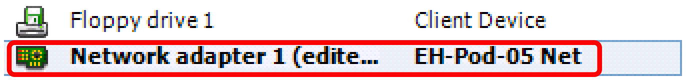
□ Quiesce guest file system (Needs VMware Tools installed)

IMPORTANT, back up your VM!

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

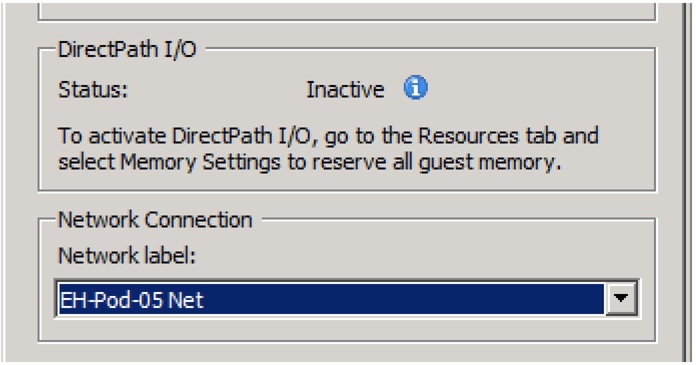
Configuring the EH-OWASP VM in EH-Pod-xx




Floppy drive 1 — Client Device

Network adapter 1 (edite... — EH-Pod-05 Net

Pod 5 example


DirectPath I/O

Status: Inactive

To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory.

Network Connection

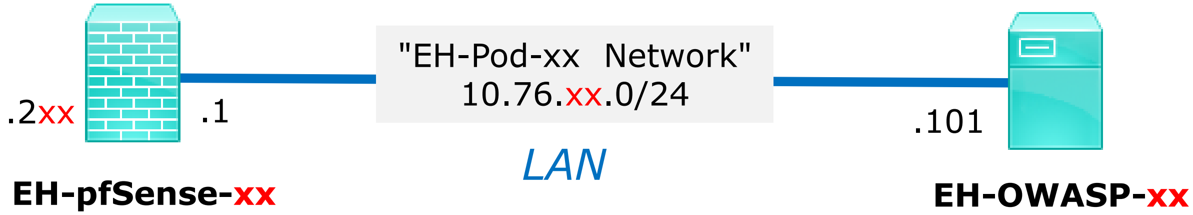
Network label: EH-Pod-05 Net

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.

Configuring the EH-OWASP VM in EH-Pod-xx



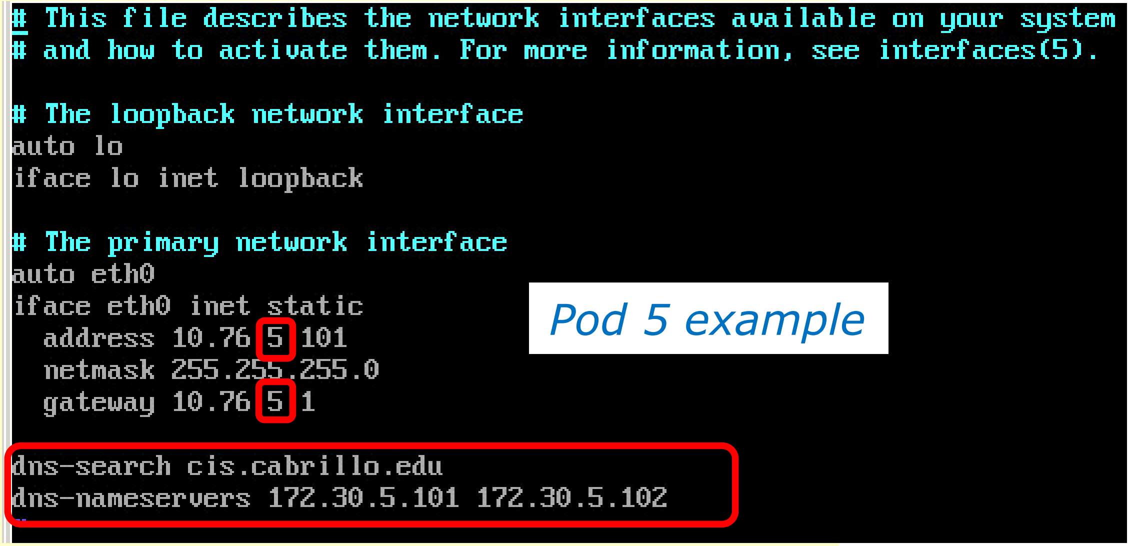
Network Configuration

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 xx.



```
# 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
```

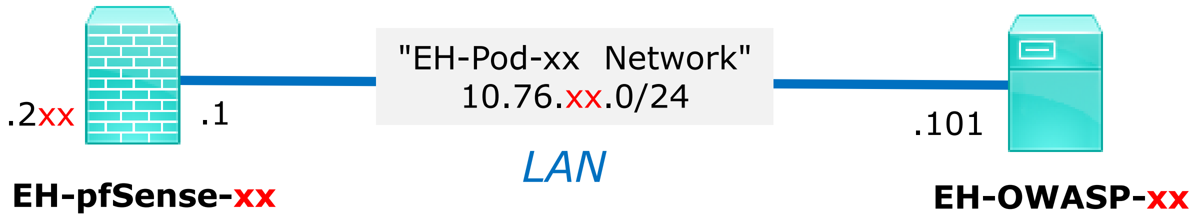
Pod 5 example

b) If missing add: **dns-search cis.cabrillo.edu**

c) If missing add: **dns-nameservers 172.30.5.101 172.30.5.102**

d) Save and exit.

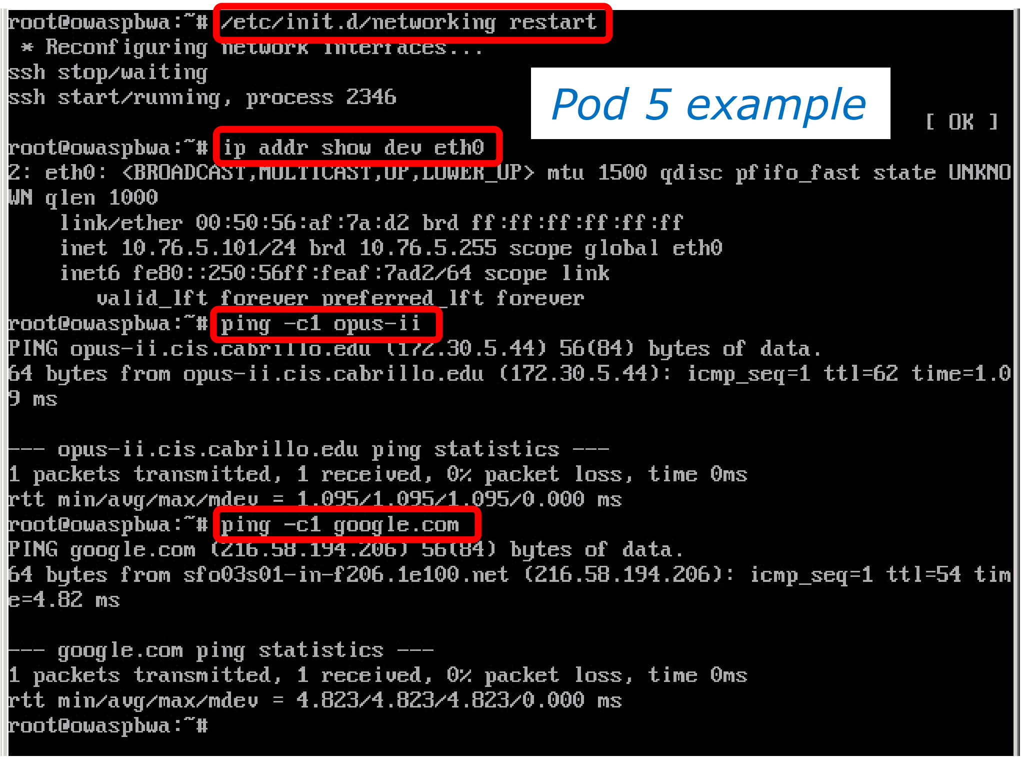
Configuring the EH-OWASP VM in EH-Pod-xx



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

5) Verify the third octet of your IP address matches your pod number xx with:
ip addr show dev eth0

6) Verify network settings on eth0 and test them by pinging opus-ii and google.com:
ping -c1 opus-ii
ping -c1 google.com

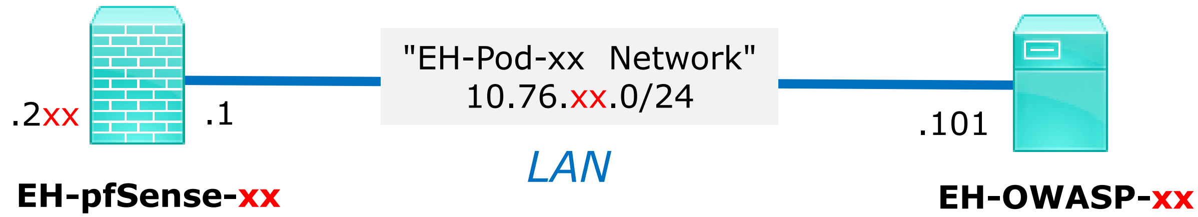


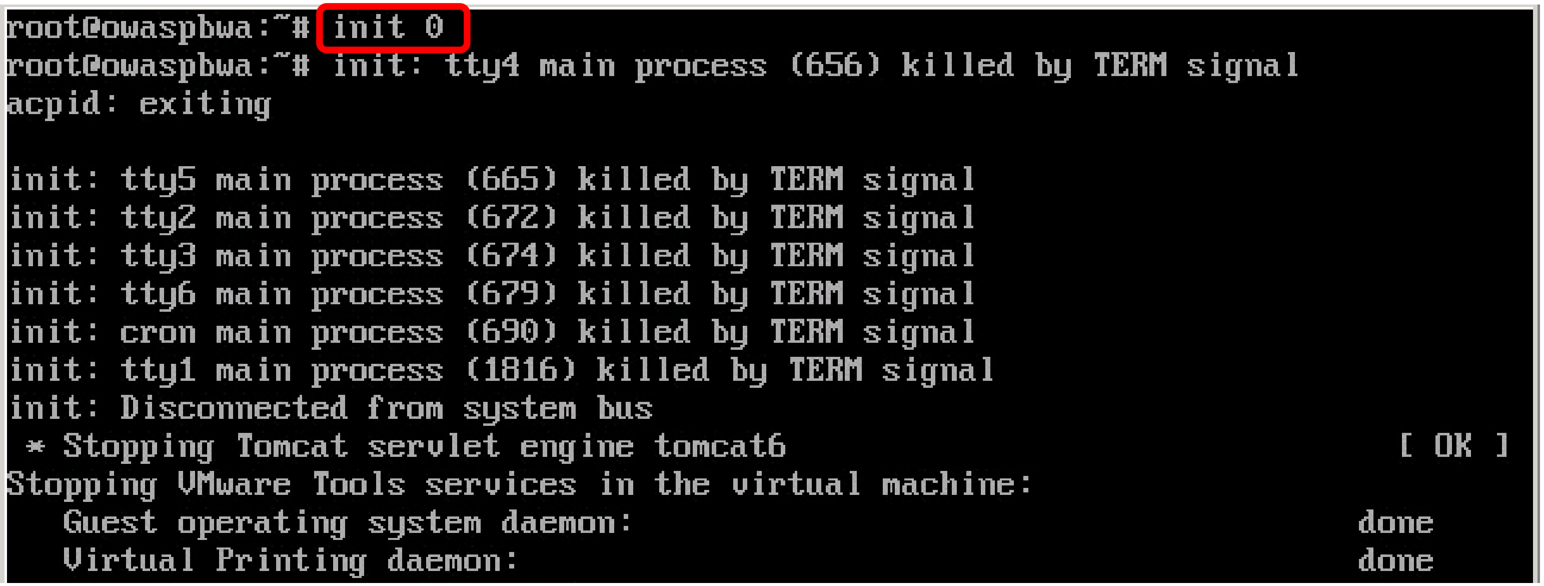
Pod 5 example

```
root@owaspbwa:~# /etc/init.d/networking restart
 * Reconfiguring network interfaces...
ssh stop/waiting
ssh start/running, process 2346
                                                                          [ OK ]
root@owaspbwa:~# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNO
WN qlen 1000
    link/ether 00:50:56:af:7a:d2 brd ff:ff:ff:ff:ff:ff
    inet 10.76.5.101/24 brd 10.76.5.255 scope global eth0
    inet6 fe80::250:56ff:feaf:7ad2/64 scope link
       valid_lft forever preferred_lft forever
root@owaspbwa:~# ping -c1 opus-ii
PING opus-ii.cis.cabrillo.edu (172.30.5.44) 56(84) bytes of data.
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=1 ttl=62 time=1.0
9 ms

--- opus-ii.cis.cabrillo.edu ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.095/1.095/1.095/0.000 ms
root@owaspbwa:~# ping -c1 google.com
PING google.com (216.58.194.206) 56(84) bytes of data.
64 bytes from sfo03s01-in-f206.1e100.net (216.58.194.206): icmp_seq=1 ttl=54 tim
e=4.82 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.823/4.823/4.823/0.000 ms
root@owaspbwa:~#
```

Note: Your EH-pfSense VM needs to be configured and running for the pings to be successful.

Configuring the EH-OWASP VM in EH-Pod-xx

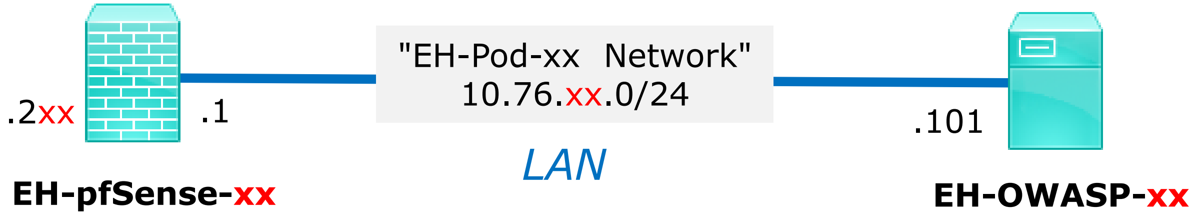




```
root@owaspbwa:~# init 0
root@owaspbwa:~# init: tty4 main process (656) killed by TERM signal
acpid: exiting

init: tty5 main process (665) killed by TERM signal
init: tty2 main process (672) killed by TERM signal
init: tty3 main process (674) killed by TERM signal
init: tty6 main process (679) killed by TERM signal
init: cron main process (690) killed by TERM signal
init: tty1 main process (1816) killed by TERM signal
init: Disconnected from system bus
 * Stopping Tomcat servlet engine tomcat6                               [ OK ]
Stopping VMware Tools services in the virtual machine:
   Guest operating system daemon:                                      done
   Virtual Printing daemon:                                            done
```

7) Shutdown VM with: **init 0**

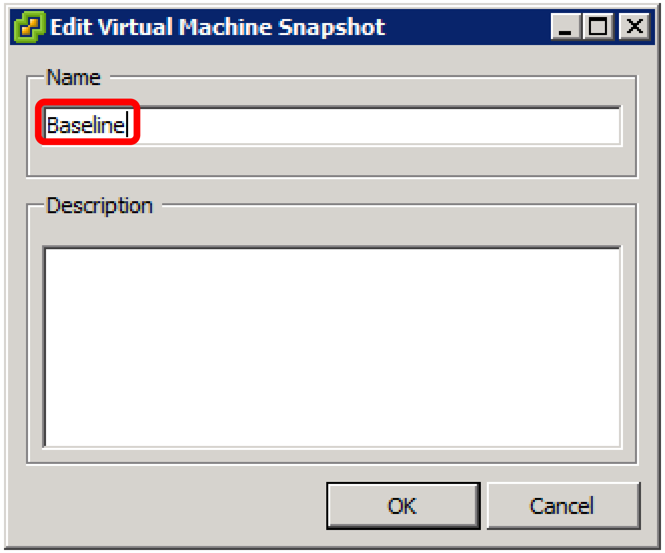
Configuring the EH-OWASP VM in EH-Pod-xx



Save your work

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

Now if you mess things up later can always start over again!



Name: Baseline

Description:

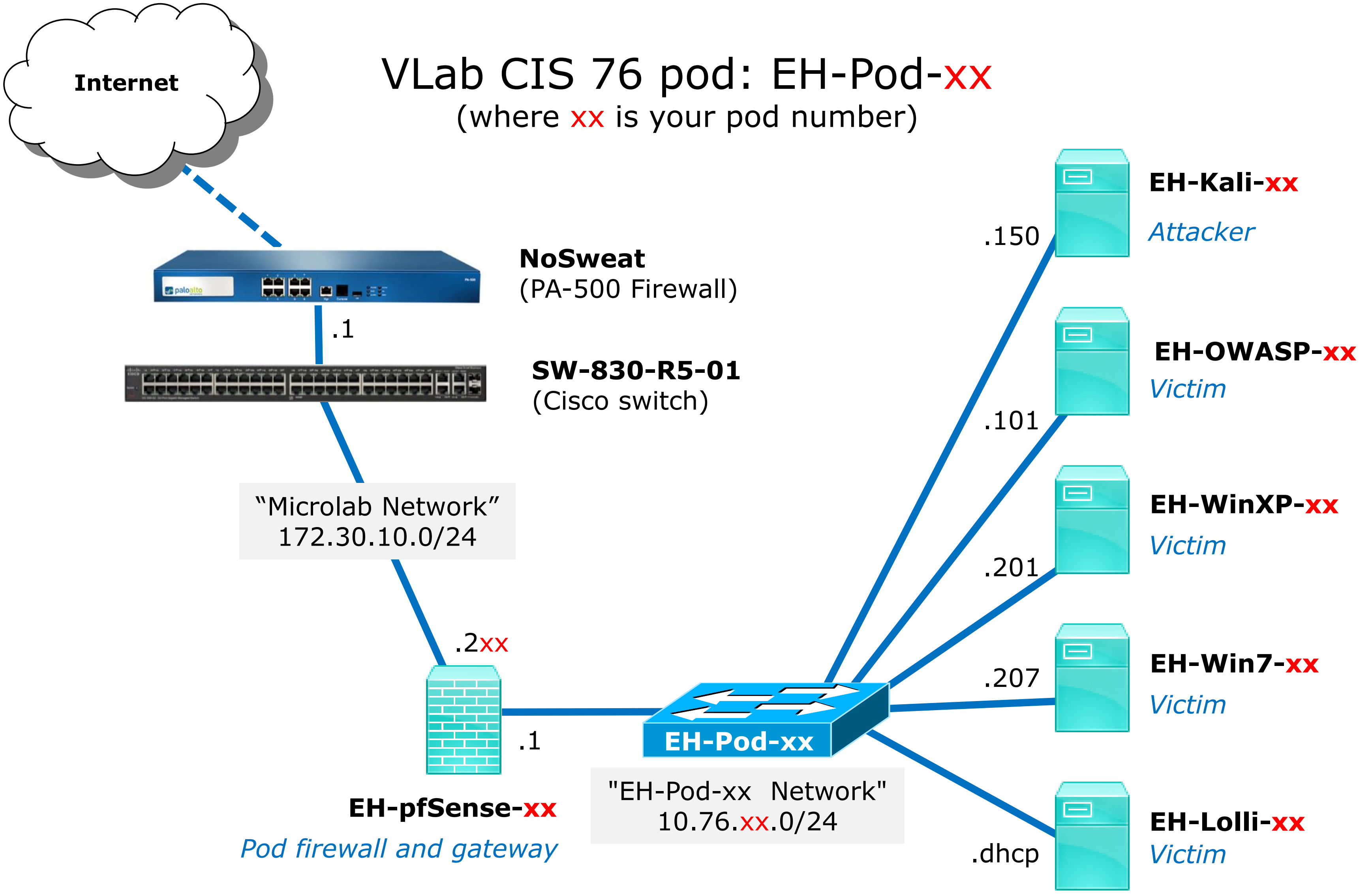
EH-Lolli-xx

VM Config

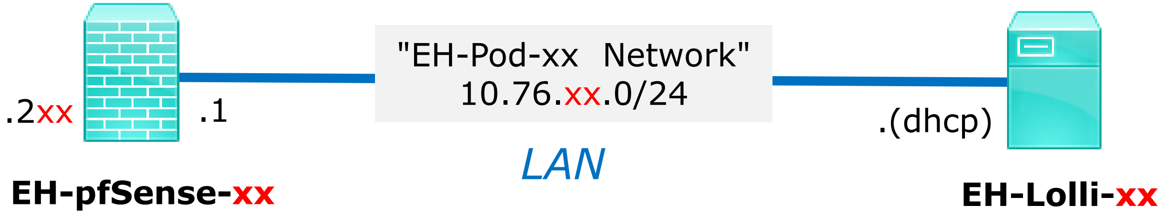
CIS 76 - VLab Pod Setup

VLab CIS 76 pod: EH-Pod-xx

(where xx is your pod number)



Configuring the Lolli VM in EH-Pod-xx

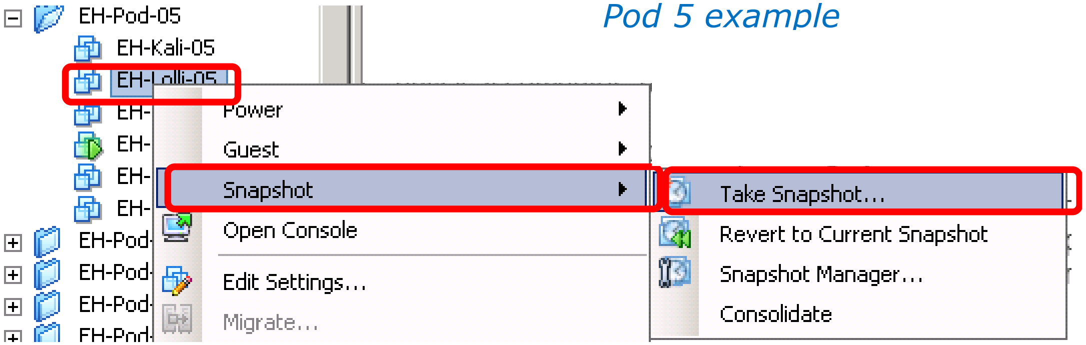


xx is the pod number assigned to you.

Lolli VM	Pod xx settings
VM Network Adapter 1	EH-Pod-xx Net

Configuring the Lolli VM in EH-Pod-05

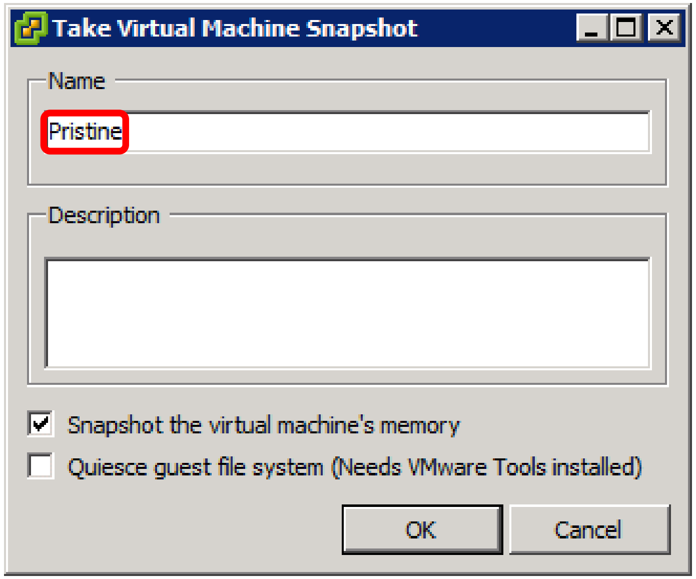
Pod 5 example



IMPORTANT, back up your VM!

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

Now if you mess things up you can always start over again!



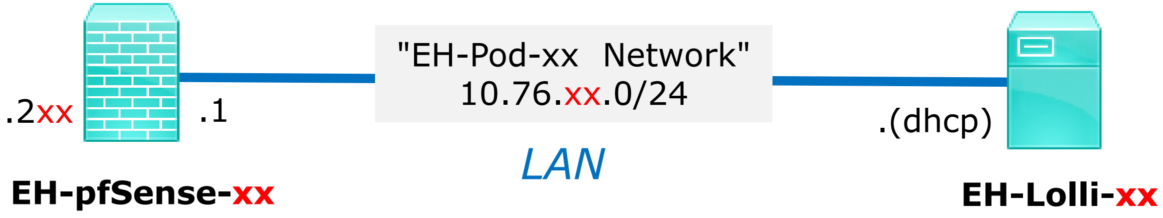
Name: Pristine

Description:

☑ Snapshot the virtual machine's memory

☐ Quiesce guest file system (Needs VMware Tools installed)

Configuring the Lolli VM in EH-Pod-xx



.2xx

.1

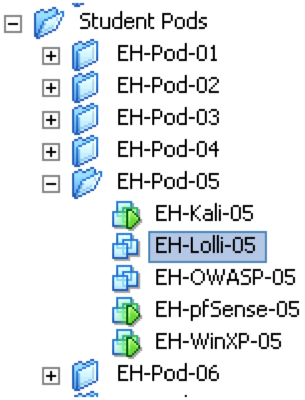
"EH-Pod-xx Network"
10.76.xx.0/24

LAN

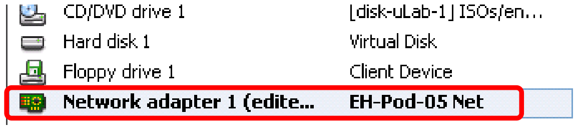
.(dhcp)

EH-pfSense-xx

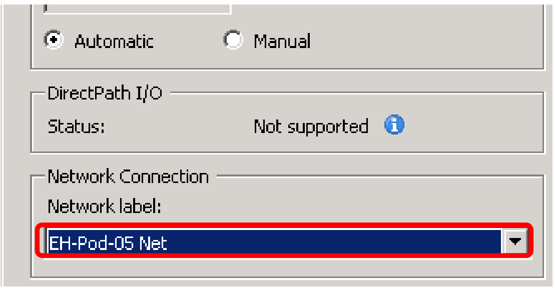
EH-Lolli-xx



- Student Pods
  - EH-Pod-01
  - EH-Pod-02
  - EH-Pod-03
  - EH-Pod-04
  - EH-Pod-05
    - EH-Kali-05
    - EH-Lolli-05
    - EH-OWASP-05
    - EH-pfSense-05
    - EH-WinXP-05
  - EH-Pod-06



CD/DVD drive 1	[disk-uLab-1] ISOs/en...
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1 (edite...	**EH-Pod-05 Net**



● Automatic ○ Manual

DirectPath I/O

Status: Not supported

Network Connection

Network label:

EH-Pod-05 Net

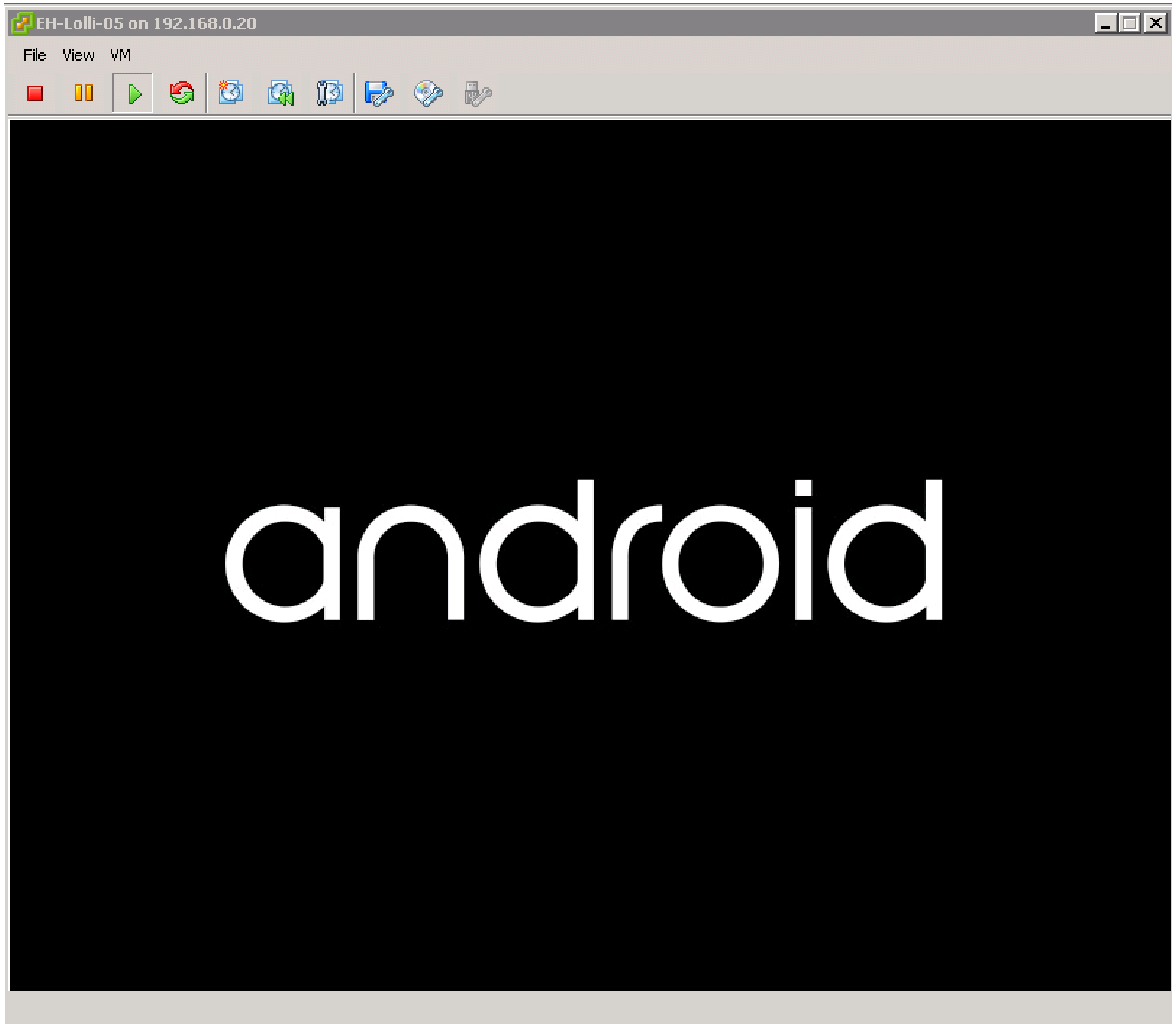
Pod 5 example

Network Cabling

1) Edit the settings of your Lolli VM.

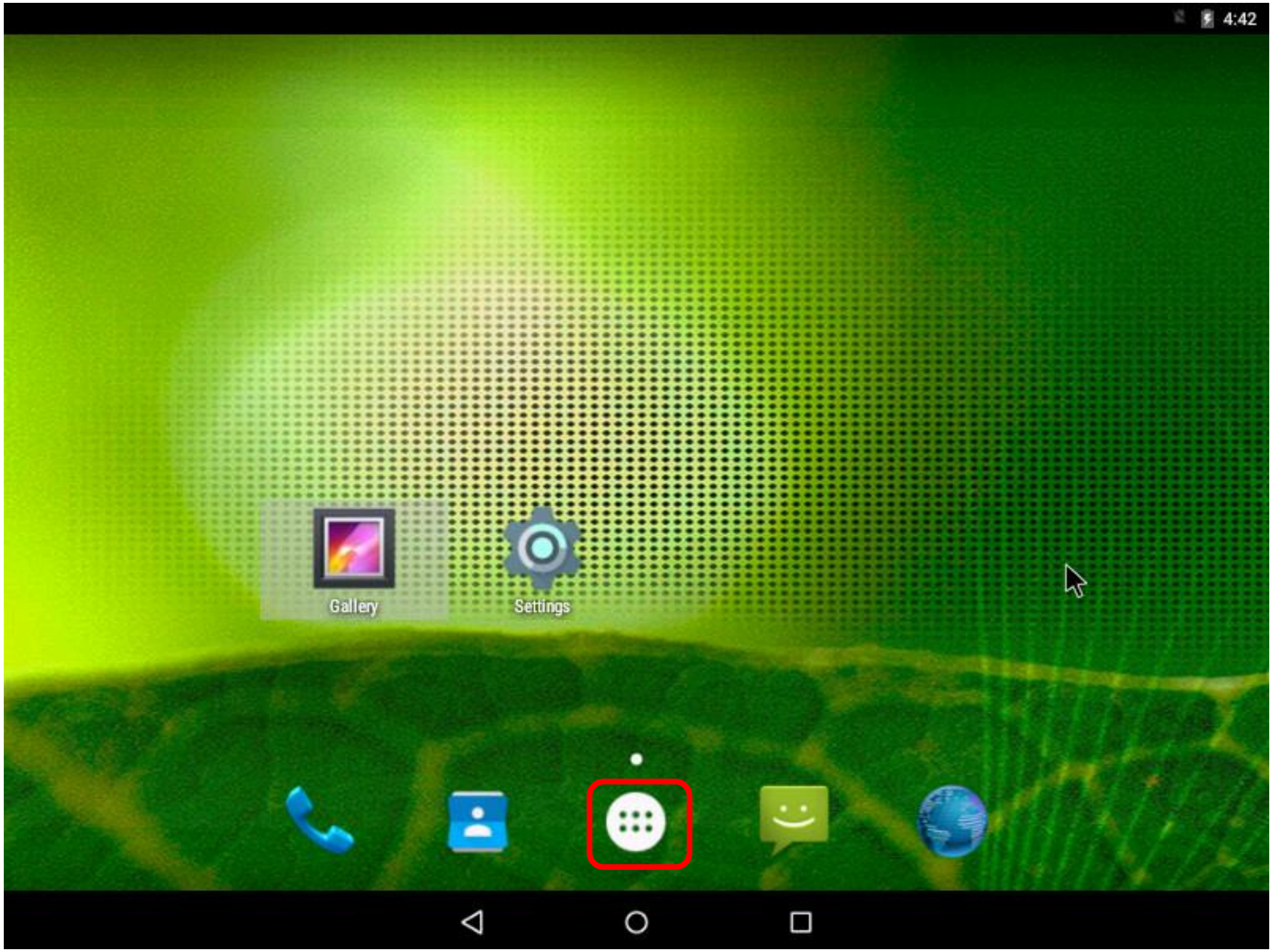
2) Network Adapter 1 should be connected to the "EH-Pod-xx Net" where xx is your pod number.

Configuring the Lolli VM in EH-Pod-05



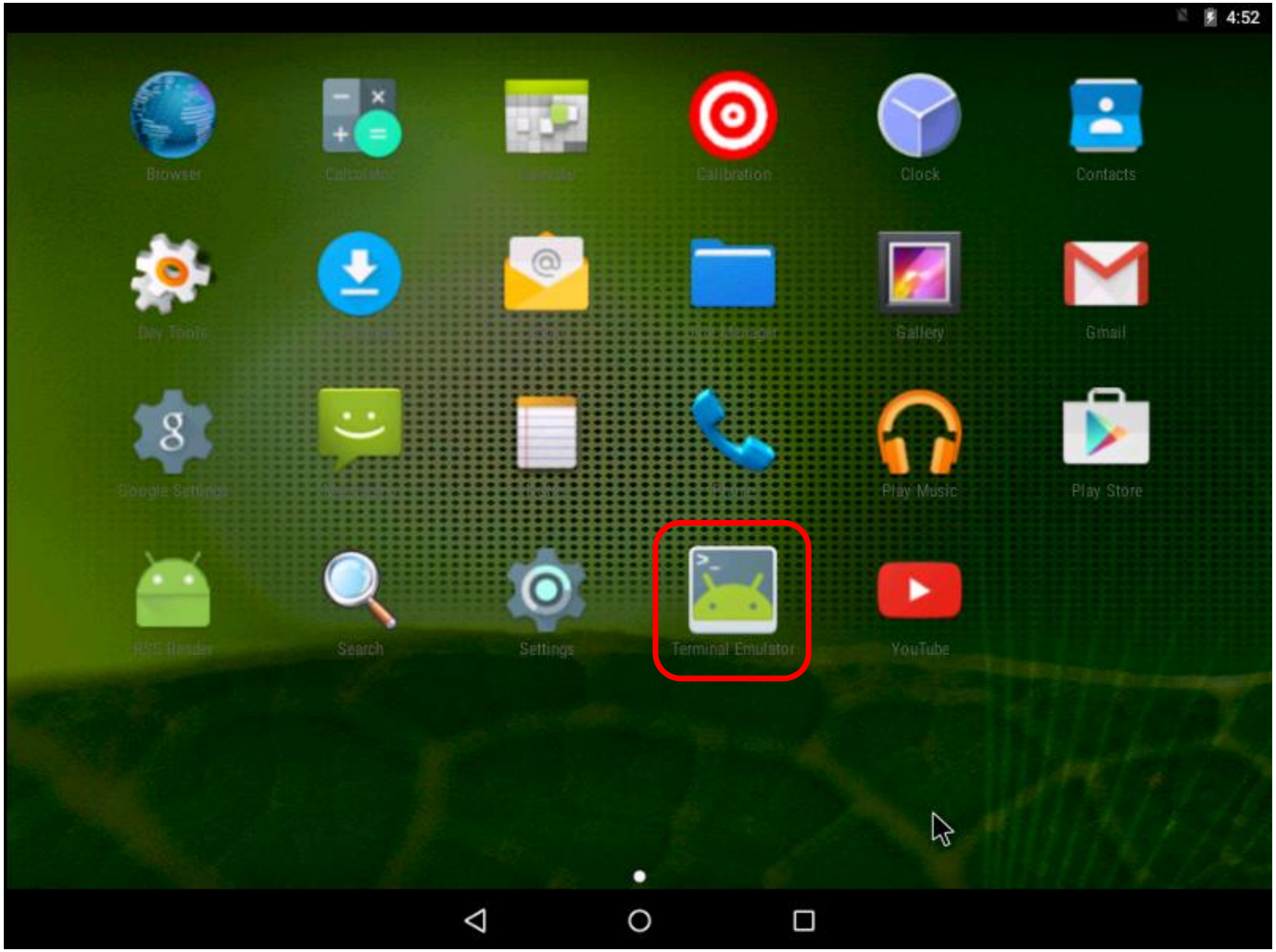
1) Power up VM and bring up a console.

Configuring the Lolli VM in EH-Pod-05



2) Click the Apps icon with the Android mouse.

Configuring the Lolli VM in EH-Pod-05

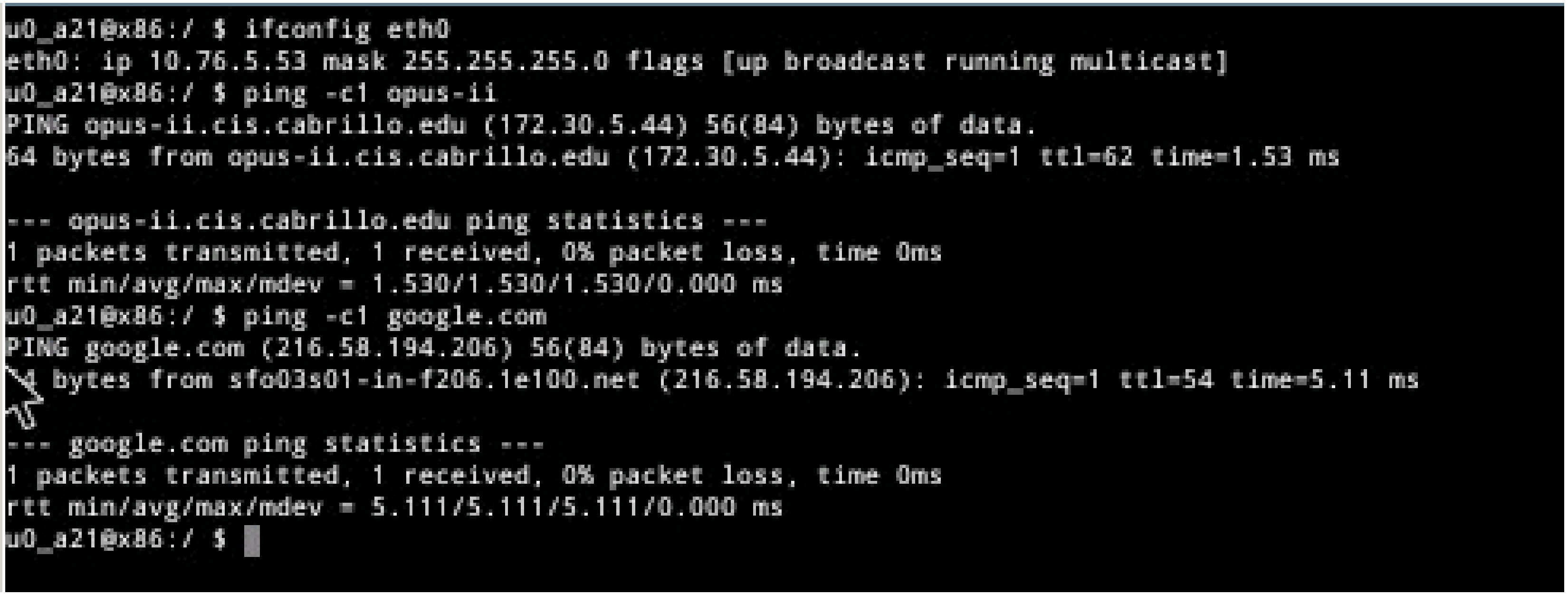


3) Click the Terminal Emulator app icon to launch it.

Configuring the Lolli VM in EH-Pod-05

3) Enter the following commands to check your network settings:

ifconfig eth0
ping -c1 opus-ii
ping -c1 google.com

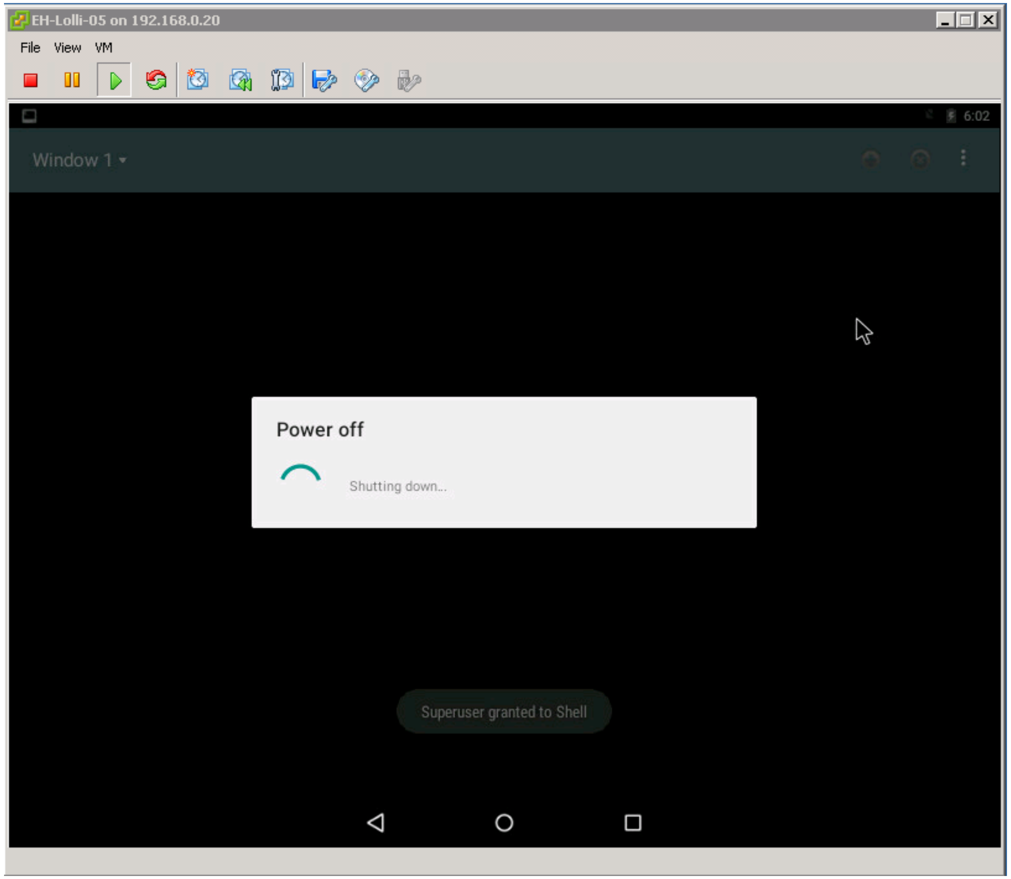


```
u0_a21@x86:/ $ ifconfig eth0
eth0: ip 10.76.5.53 mask 255.255.255.0 flags [up broadcast running multicast]
u0_a21@x86:/ $ ping -c1 opus-ii
PING opus-ii.cis.cabrillo.edu (172.30.5.44) 56(84) bytes of data.
64 bytes from opus-ii.cis.cabrillo.edu (172.30.5.44): icmp_seq=1 ttl=62 time=1.53 ms

--- opus-ii.cis.cabrillo.edu ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.530/1.530/1.530/0.000 ms
u0_a21@x86:/ $ ping -c1 google.com
PING google.com (216.58.194.206) 56(84) bytes of data.
64 bytes from sfo03s01-in-f206.1e100.net (216.58.194.206): icmp_seq=1 ttl=54 time=5.11 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 5.111/5.111/5.111/0.000 ms
u0_a21@x86:/ $
```

Check that your EH-Lolli-xx VM got an IP address from your EH-pfSense-xx VM and has network connectivity.

```
adb shell su -c 'svc power shutdown'
```

Configuring the Lolli VM in EH-Pod-05



EH-Lolli-05 on 192.168.0.20

Power off

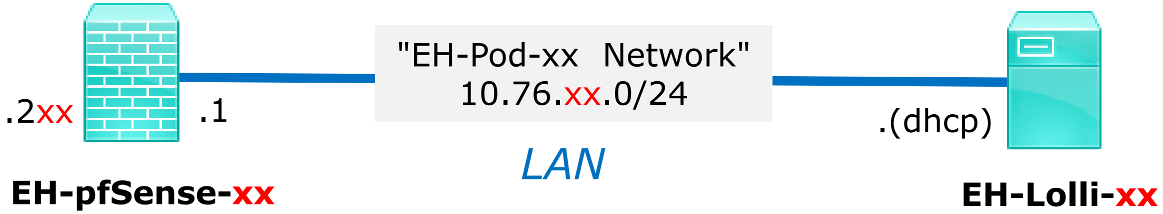
Shutting down...

Superuser granted to Shell

3) To shutdown android enter:

adb shell su -c 'svc power shutdown'

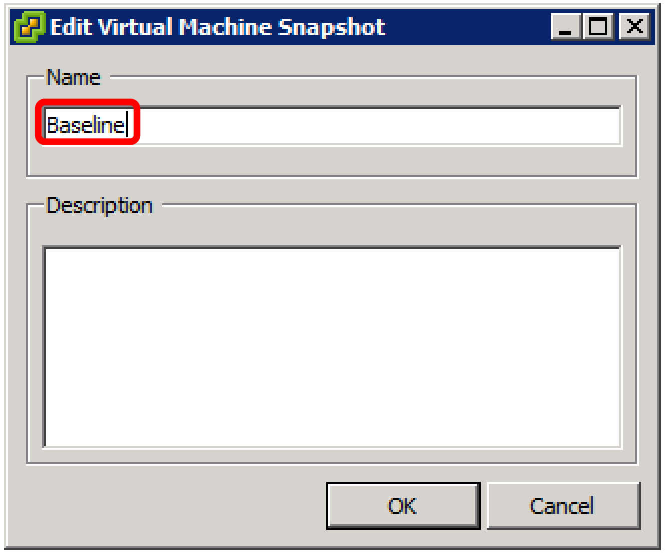
Configuring the Lolli VM in EH-Pod-xx



Save your work

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

Now if you mess things up later can always start over again!



Name

Baseline

Description