BI-SSB - Lab Manual 2
Install ASA5505 in GNS3, with software version 9

1. Introduction

The network topology remains the same as in the previous lab, with the three zones: inside, outside and DMZ. The only change is the fact that the former router BORDER is now replaced with an ASA5505 device.

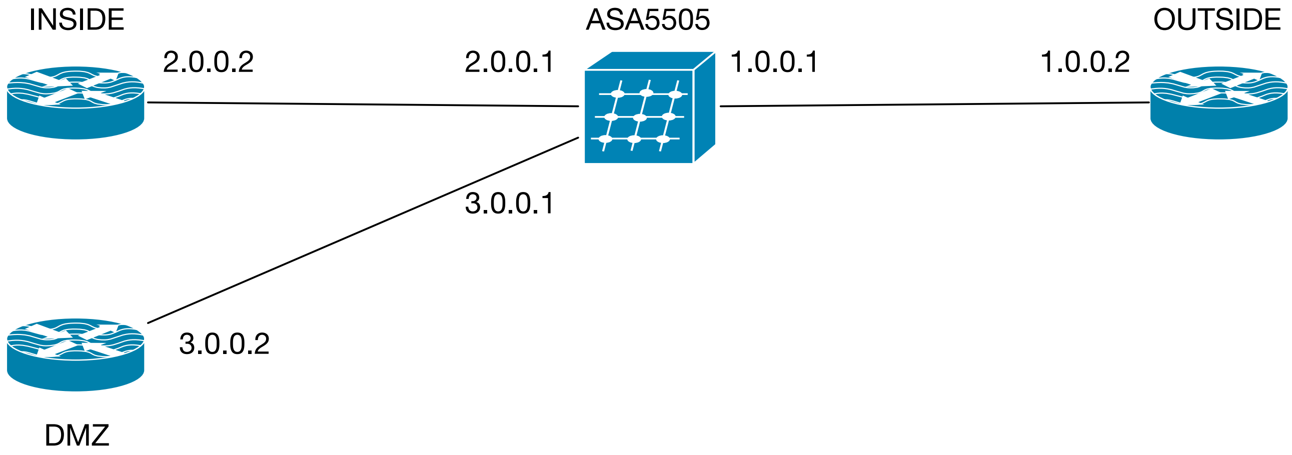


Figure 1 - The diagram of the network

In this diagram all the masks are supposed to be /8, thus 255.0.0.0 and thus any needed wildcard (inverted mask) will be 0.255.255.255. The routers BORDER, INSIDE and DMZ are supposed to belong to out company while the OUTSIDE router is supposed to belong to the ISP (Internet Service Provider).

The terms “inbound” and “outbound” are referred from the perspective of our company, thus inbound traffic is traffic from OUTSIDE to any other router. Outbound traffic is traffic from any router to OUTSIDE.

The terms “incoming” and “outgoing” are referred to a router, representing traffic coming to and respectively going from that particular router. Thus, from the perspective of router BORDER, incoming traffic may be from any other router in the topology and outgoing traffic is towards any other router of the topology.

2. Installation of ASA5505 with software version 9

ASA5505 is a device which smells Cisco, looks Cisco but in fact it is a Cisco operating system running on top of a Linux operating system. Thus it means that even in hardware ASA OS is in fact virtualised. This makes it extremely installable on other systems. In fact, by doing what I present here you may have an ASA5505 at home. I do have it in hardware (real device) but the virtualised one behaves 100% the same.

ASA is a system which strongly depends on two parameters: the hardware platform (how powerful it is) and license. The license for the ASA5505 allows for 3 zones around the device, for 3 networks. Of course we may use the ones which we have previously defined (inside, outside and DMZ) but ASA is configurable in graphical interface using a tool which is called ASDM. What we are going to do is to eliminate the DMZ zone and instead we shall put the CONFIG zone which is a separated network for only configuring the ASA. On that zone we shall install a Windows XP machine which has installed the ASDM. The zone will be in a private subnet which will not be routed (it is used for configuring only). We may have put the computer on the INSIDE but I wanted to present you dedicated subnets for configuration (out of channel configuration).

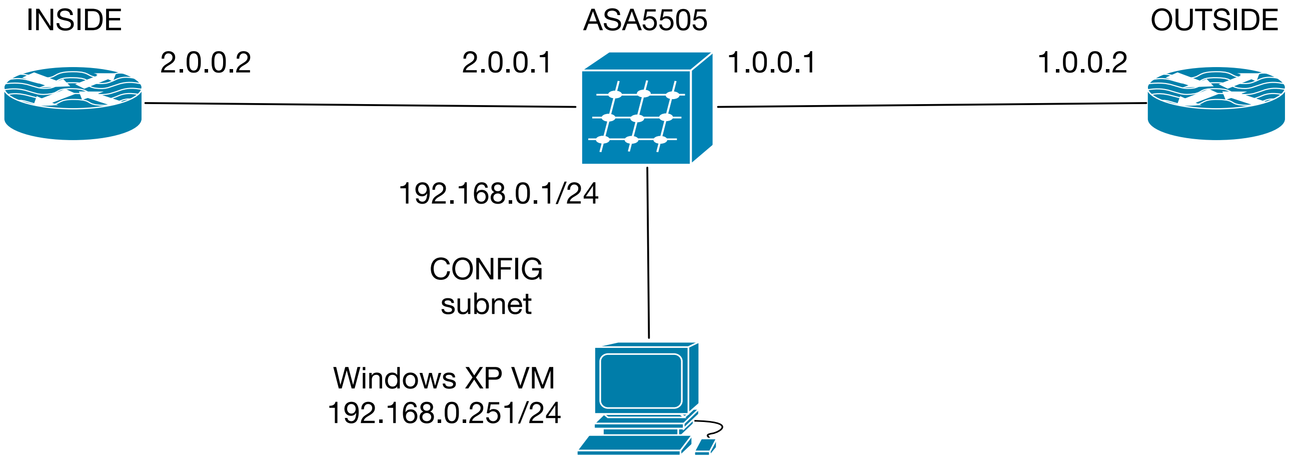


Figure 2 - The diagram of the network

2.1 Installing the QEMU software

You need to install QEMU. I do not know how it is done on your operating system. On MacOS you need to install Macports (https://www.macports.org) and then install QEMU by typing: *sudo port install qemu*. You have to find the appropriate way to install QEMU on your system. You need version 2.10 or higher 64 bit recommended. It may work on 32 bit but I have no idea. Strange sentence for a teacher who must show things. I am a specialist and it means I know in detail only few things :) More, I do not have to understand or remember everything - that is the task for students. A doctor only needs to know where are the books. The job of a docent is to know where are the doctors and the job of a professor is to know where are the docents :)

After you install QEMU you can now install ASA.

ALWAYS give root access to uBridge from GNS3!!!

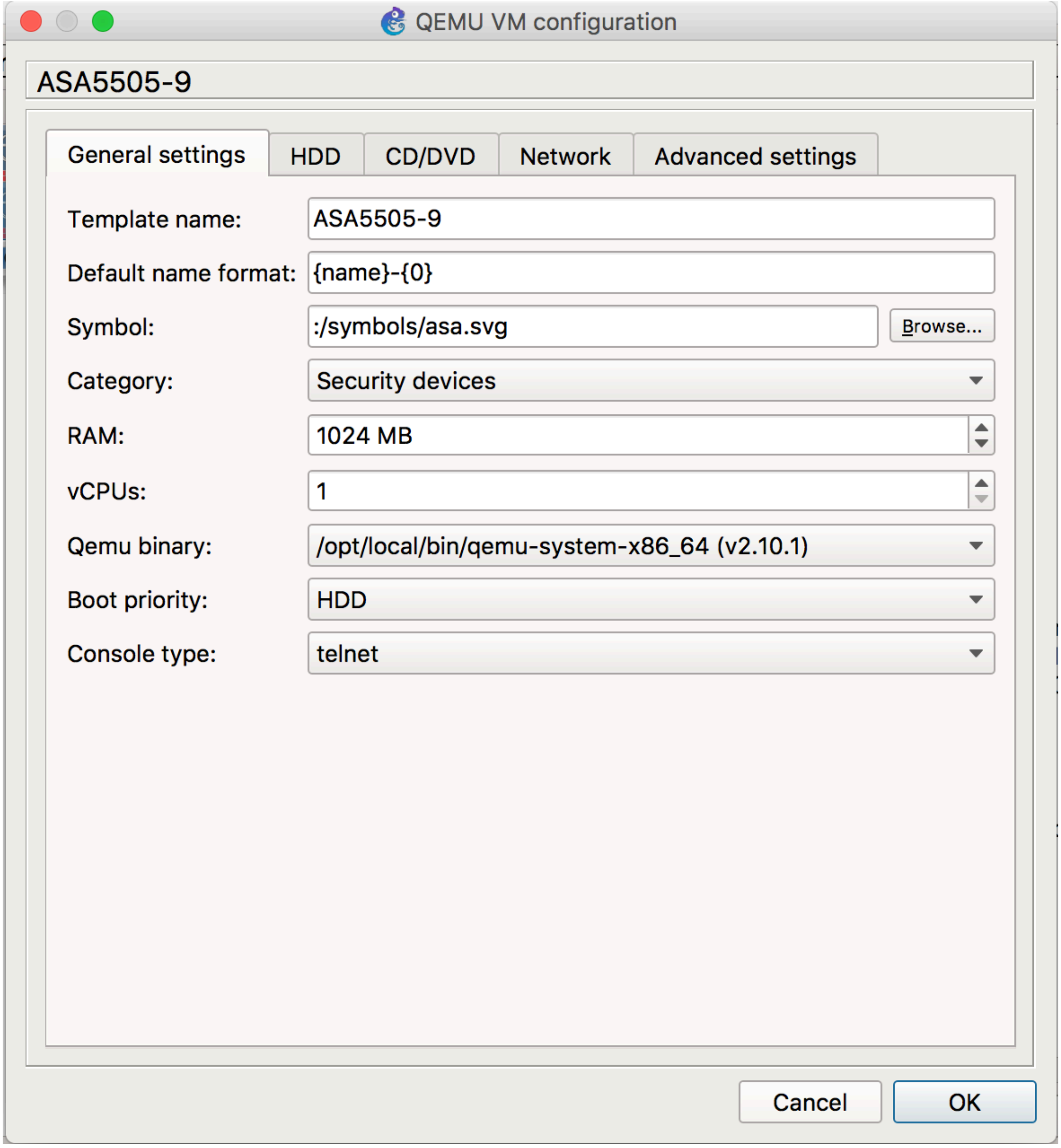
2.2 Installing the ASA5505

Go to https://moucha.org/bissb-2017/ASA5505.zip and download the archive. It has 28 MB but when you decompress it it will have around 550 MB. It contains 6 files from which 3 are the MD5 hashes of the other three. Copy the files on your GNS3 project location under the folder QEMU. Usually it is under GNS3 / images / QEMU.

Open GNS3 and go to Preferences -> QemuVMs and click New.

- Put the name of the device ASA5505-9. Click Next.

- Select the QEMU binary. Mine is /opt/local/bin/qemu-system-x86_64 (v2.10.1). Give it 1024 MB RAM. Click Next.
- Leave telnet. Click Next.
- Disk image: select the file FLASH which you copied. This acts as a saving storage for your device and emulates the CF card inside the ASA5505. Without this, the ASA will not be able to save anything. The size which you have is 512 MB. In my house the device has 4 GB (as a fact). Next.
- Click finish. Do not worry, you did not finish yet. We now edit the settings. Click Edit.
- BE SURE TO HAVE IDENTICAL OR SIMILAR SETTINGS!!!



ASA5505-9

Template name: ASA5505-9

Default name format: {name}-{0}

Symbol: :/symbols/asa.svg

Category: Security devices

RAM: 1024 MB

vCPUs: 1

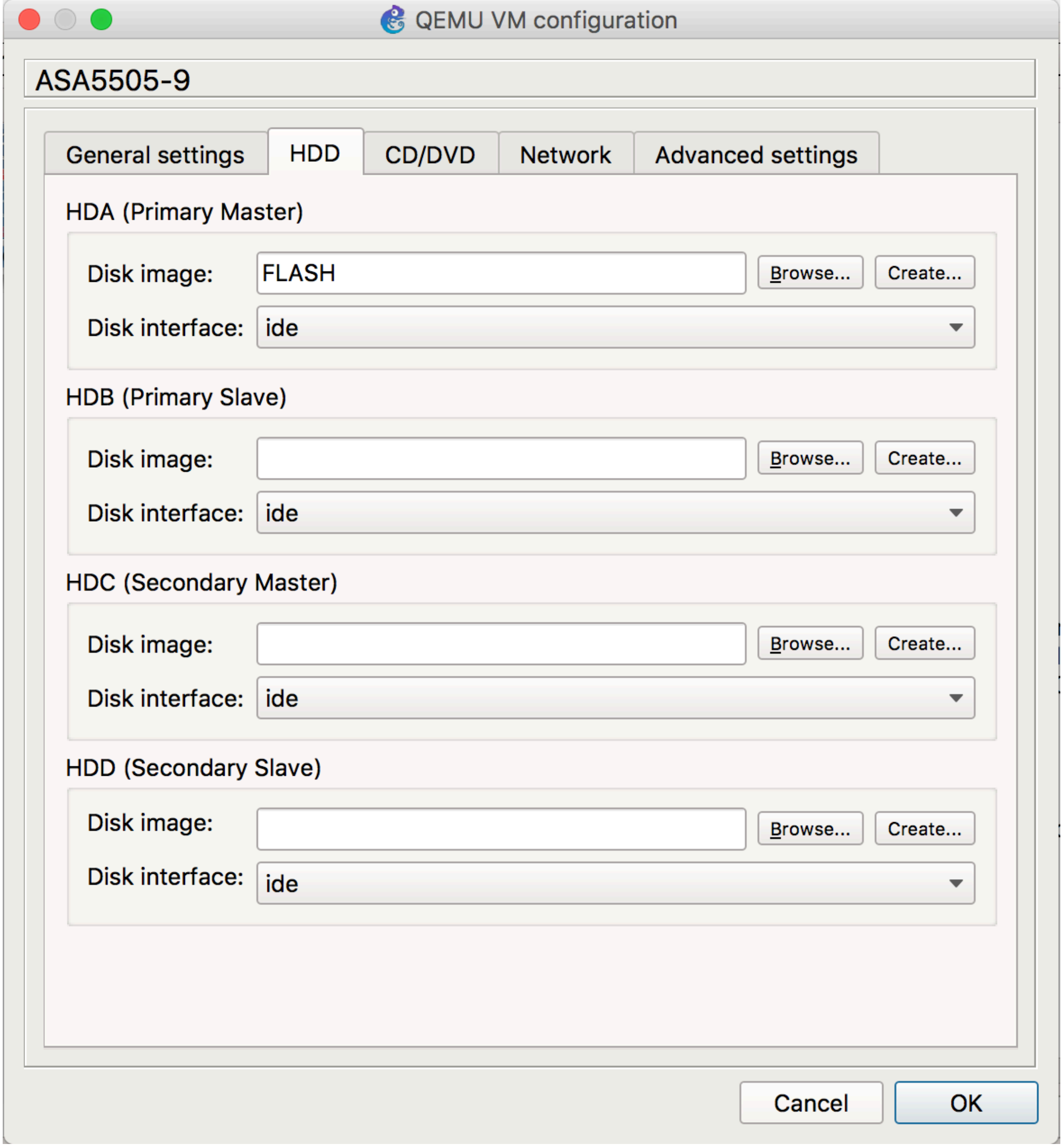
Qemu binary: /opt/local/bin/qemu-system-x86_64 (v2.10.1)

Boot priority: HDD

Console type: telnet

Figure 3 - General settings:

What I had to set was: choose category as security device, choose symbol as ASA. The rest were ok but on your machine be sure you have the proper settings of QEMU, etc.



QEMU VM configuration

ASA5505-9

HDA (Primary Master)

Disk image: FLASH

Disk interface: ide

HDB (Primary Slave)

Disk image:

Disk interface: ide

HDC (Secondary Master)

Disk image:

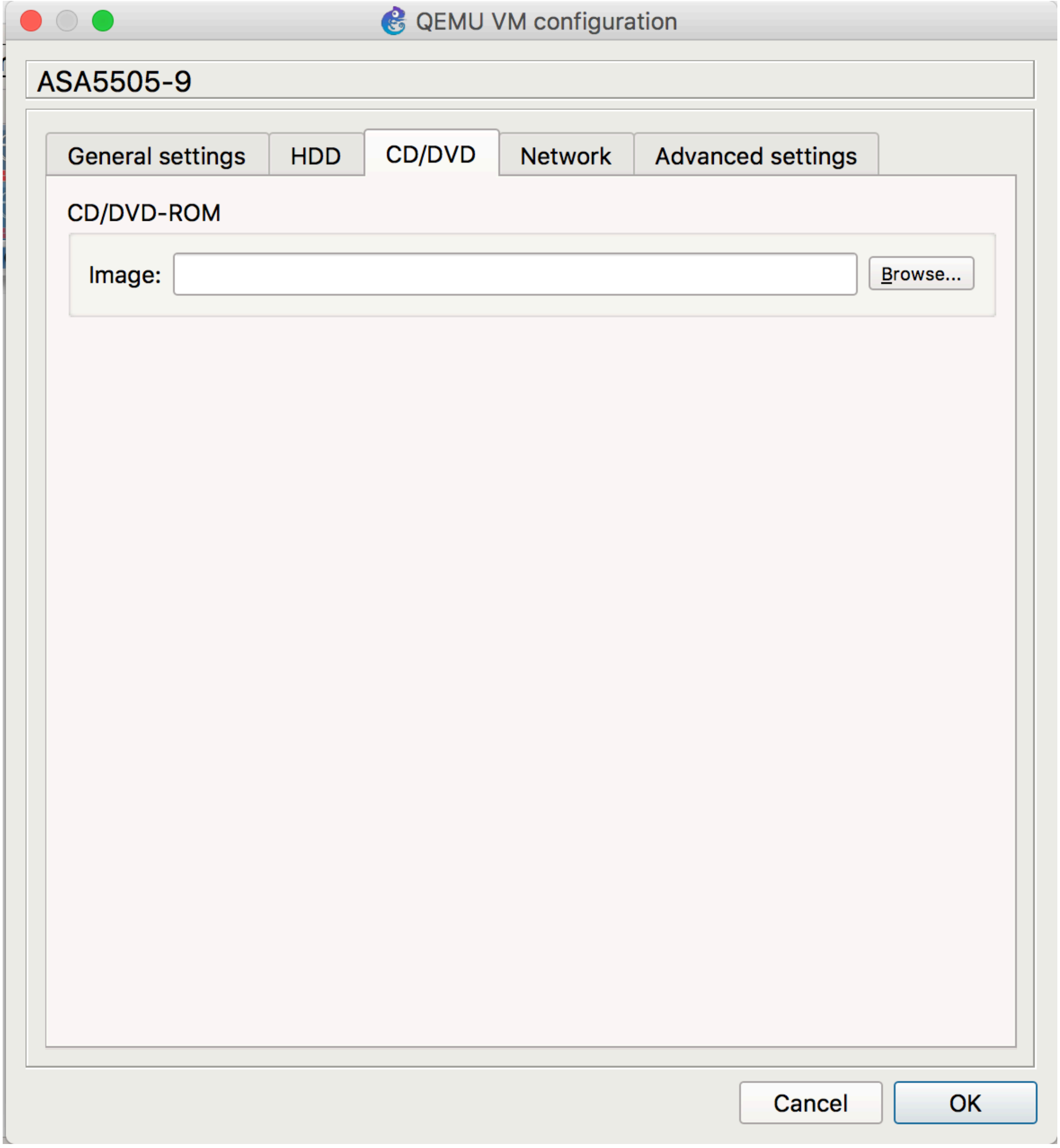
Disk interface: ide

HDD (Secondary Slave)

Disk image:

Disk interface: ide

Figure 4 - HDD - nothing to set (FLASH should be there):

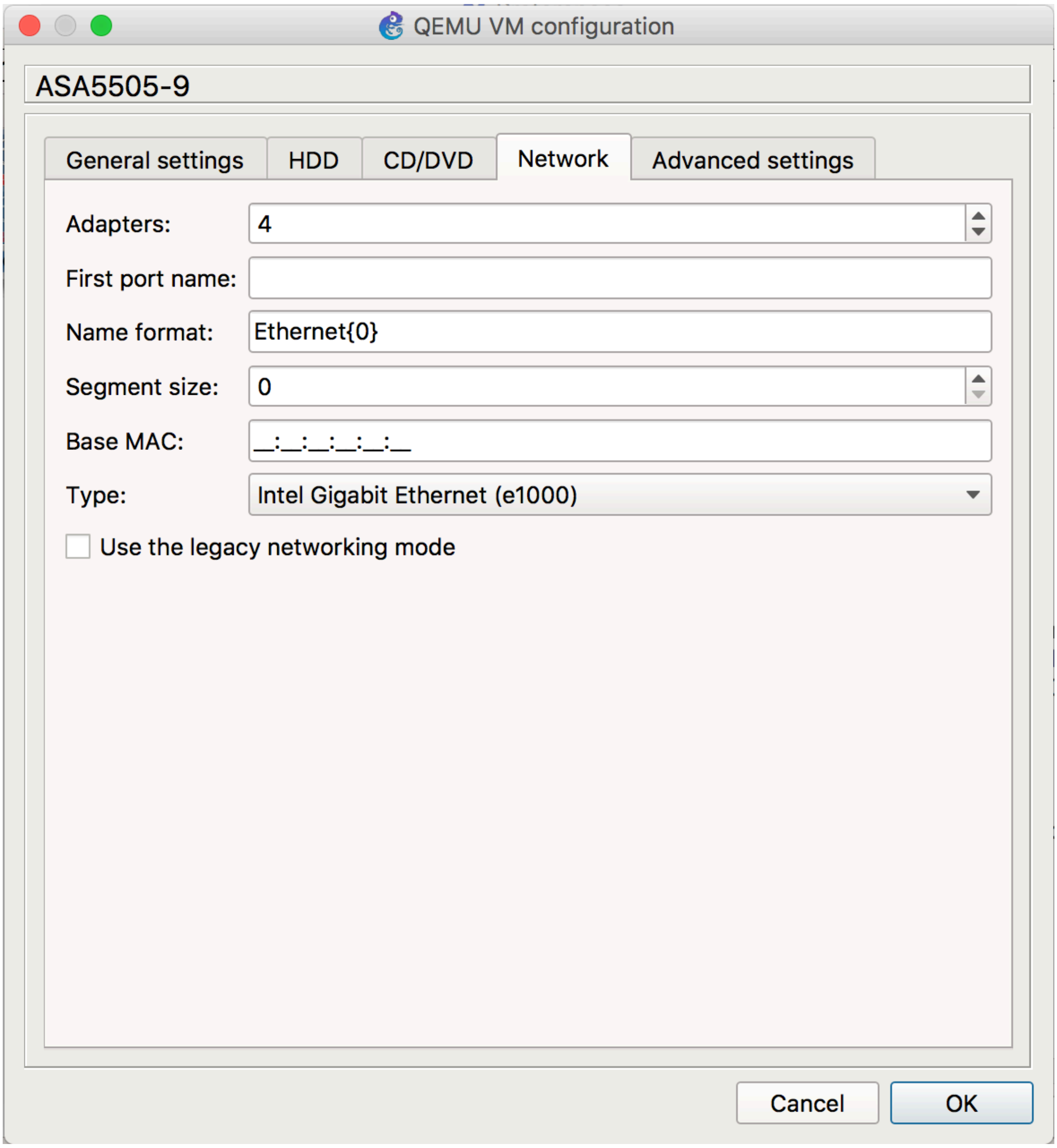


ASA5505-9

CD/DVD-ROM

Image:

Figure 5 - CD/DVD - nothing to set:



QEMU VM configuration

ASA5505-9

Adapters: 4

First port name:

Name format: Ethernet{0}

Segment size: 0

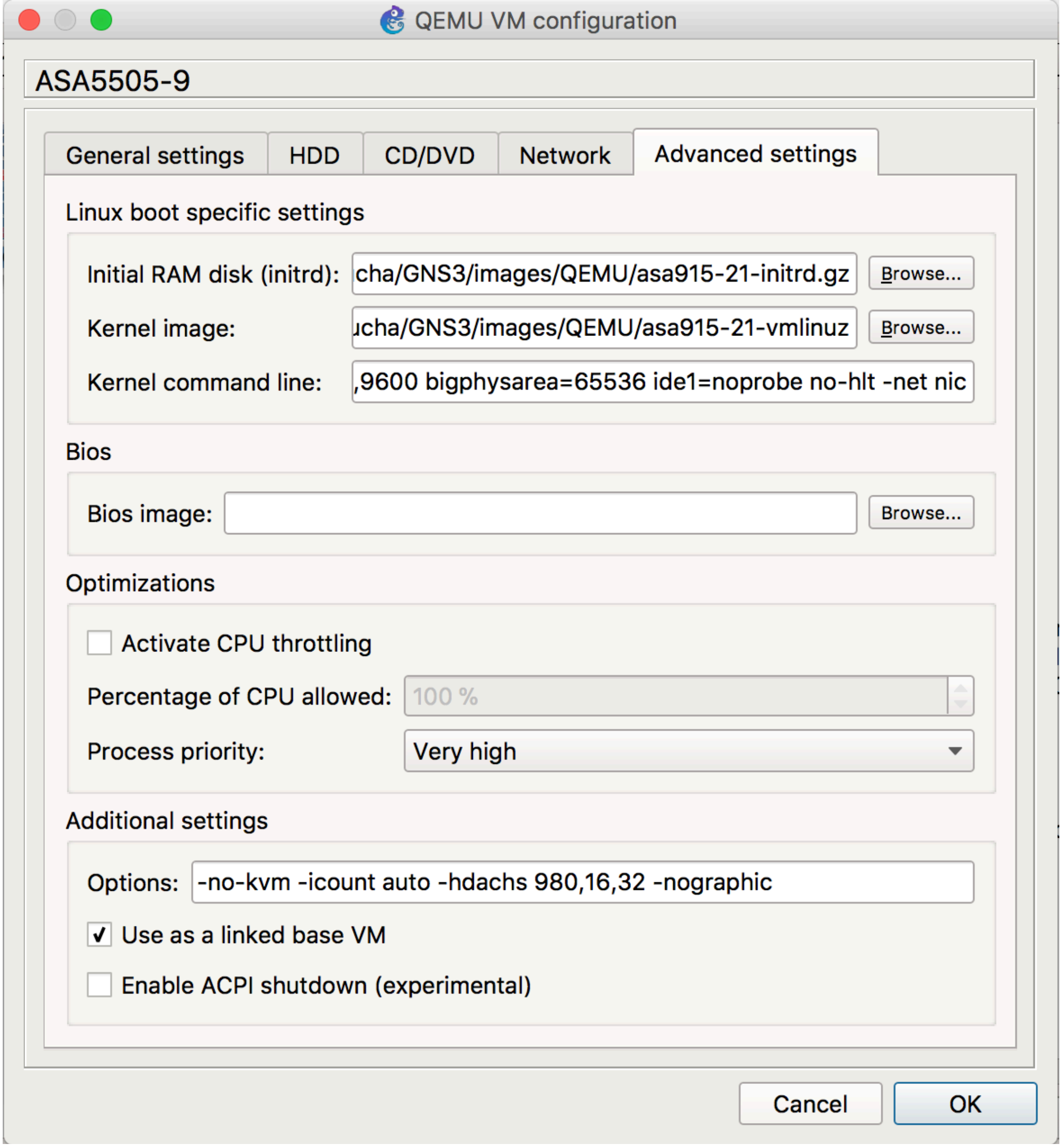
Base MAC: __:__:__:__:__:__

Type: Intel Gigabit Ethernet (e1000)

□ Use the legacy networking mode

Figure 6 - Network:

What I had to set up on my computer were: 4 network cards instead of 1.



Linux boot specific settings

Initial RAM disk (initrd): cha/GNS3/images/QEMU/asa915-21-initrd.gz

Kernel image: ıcha/GNS3/images/QEMU/asa915-21-vmlinuz

Kernel command line: ,9600 bigphysarea=65536 ide1=noprobe no-hlt -net nic

Bios

Bios image:

Optimizations

□ Activate CPU throttling

Percentage of CPU allowed: 100 %

Process priority: Very high

Additional settings

Options: -no-kvm -icount auto -hdachs 980,16,32 -nographic

☑ Use as a linked base VM

□ Enable ACPI shutdown (experimental)

Figure 7 - Advanced settings (a lot to set up):

What I set up on my computer:

Initrd image: asa915-21-initrd.gz - point it to your downloaded file

Kernel image: asa915-21-vmlinuz - point it to your downloaded file

Kernel command line: ide_generic.probe_mask=0x01 ide_core.chs=0.0:980,16,32 auto nousb console=ttyS0,9600 bigphysarea=65536 ide1=noprobe no-hlt -net nic

Options: -no-kvm -icount auto -hdachs 980,16,32 -nographic

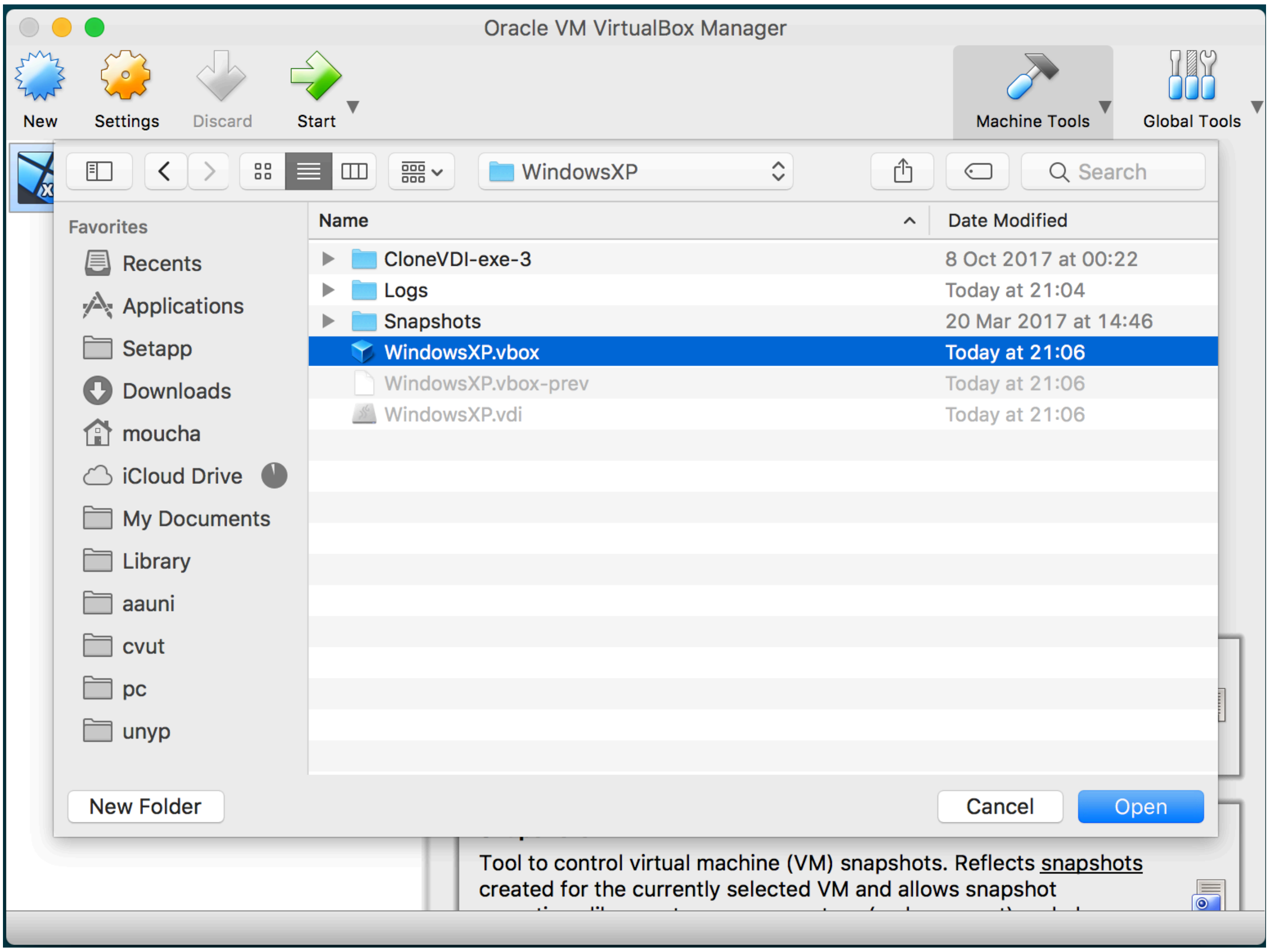
2.3 - Installing the Windows XP to VirtualBox and GNS3

Ask it from your teacher. Copy the VirtualBox virtual machine on your hard drive.

Be sure you have VirtualBox installed on your computer, including the EXTENSION PACK: https://www.virtualbox.org

Open VirtualBox, click Machine, click Add and add the WindowsXP.vbox from me.

DO NOT START THE MACHINE !!! Not necessary.

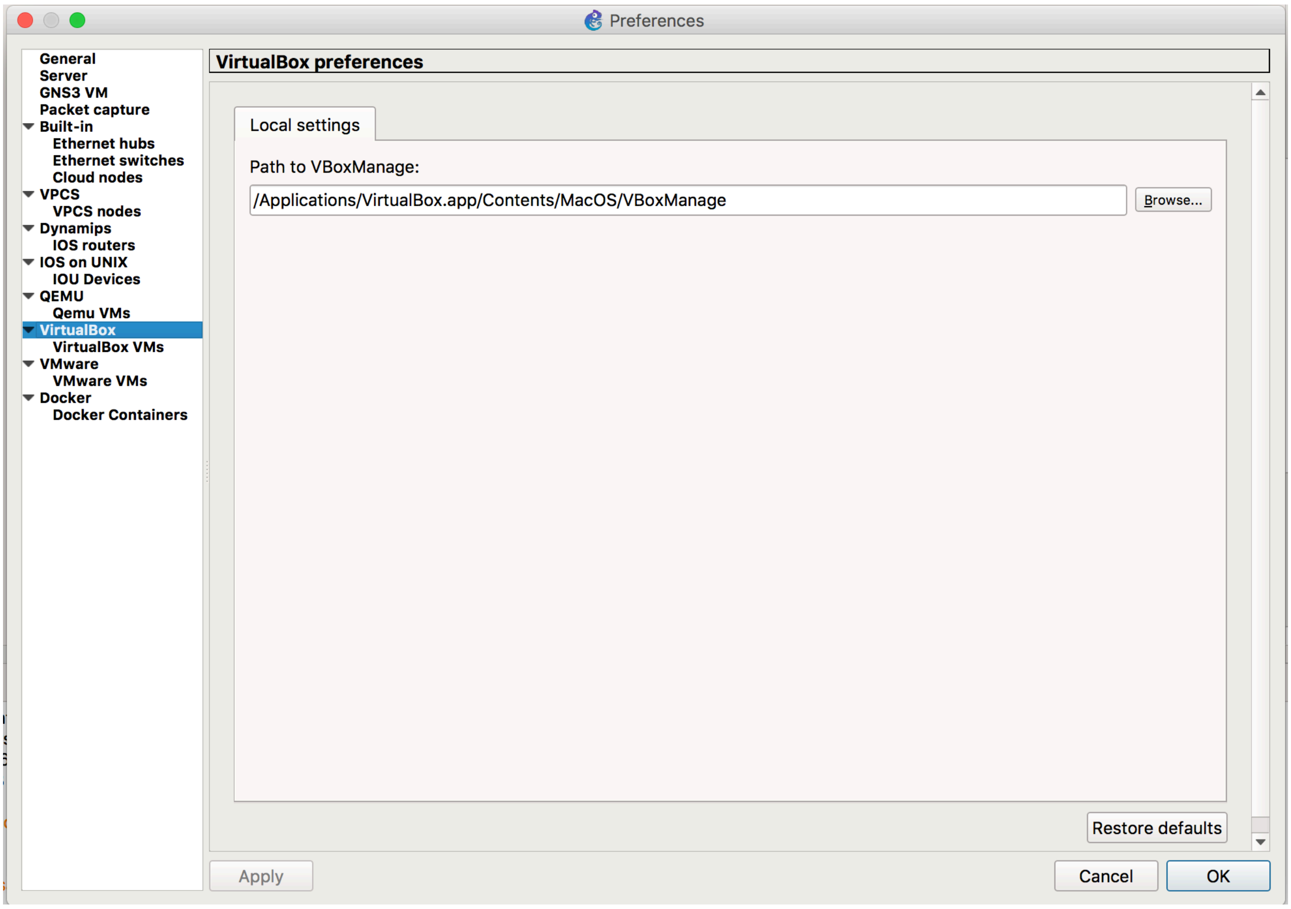


Name	Date Modified
CloneVDI-exe-3	8 Oct 2017 at 00:22
Logs	Today at 21:04
Snapshots	20 Mar 2017 at 14:46
WindowsXP.vbox	Today at 21:06
WindowsXP.vbox-prev	Today at 21:06
WindowsXP.vdi	Today at 21:06

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot

Figure 8 - Adding Windows XP to VirtualBox

Open GNS3. Go to preferences and verify VirtualBox is recognised.

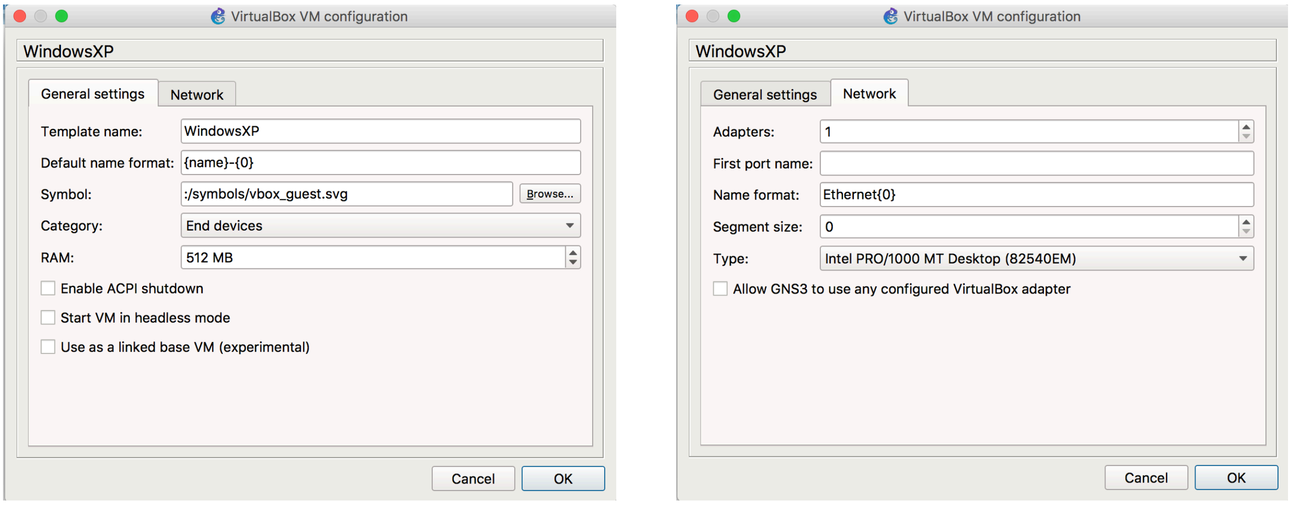


VirtualBox preferences

Path to VBoxManage: /Applications/VirtualBox.app/Contents/MacOS/VBoxManage

Figure 9 - Verify the fact that GNS3 knows VirtualBox.

Now add the XP machine to GNS3. Go one step below VirtualBox menu in the Preferences of GNS3 and click VirtualBox VMs. Click New. The XP machine should be recognised automatically. Click Finish. Verify the settings:



WindowsXP

Template name: WindowsXP

Default name format: {name}-{0}

Symbol: :/symbols/vbox_guest.svg

Category: End devices

RAM: 512 MB

☐ Enable ACPI shutdown

☐ Start VM in headless mode

☐ Use as a linked base VM (experimental)

WindowsXP

Adapters: 1

First port name:

Name format: Ethernet{0}

Segment size: 0

Type: Intel PRO/1000 MT Desktop (82540EM)

☐ Allow GNS3 to use any configured VirtualBox adapter

Figure 10 a and b - The settings of XP.

3. The first network

The first network contains only the essential parts: the Windows XP machine with the ASDM and the ASA5505. I shall give you the network. Just start it and see if it works.

Download the ASA5505 project: https://moucha.org/bissb-2017/ASA5505-9-ASDM.zip

Uncompress it and move it to your GNS3 projects folder. Keep the zip as a backup.

Enter the ASA5505-9-ASDM directory and open ASA5505-9-ASDM.gns3

The project should open. Click the PLAY button to start the devices.

To open the ASA settings, double click the ASA, type *enable* (ena) and give the password "*cisco*", which is the default password for ASA devices. You can also verify the IP address settings by typing:

```
ASA# show interface ip brief
```

Or

```
ASA# ip int ip br                //the shorthand format of the same command.
```

//Yes, on routers it is *show ip interface brief* and on ASA is *show interface ip brief*. Ask Cisco why.

Check the IP address and the interface connected to the XP machine. You should be able to ping between the XP and the ASA.

4. The first ASDM operation

ASA is a "trust based firewall" (TBFW). Each interface or zone is defined a trust level between 0 (totally untrusted) and 100 (totally trusted). Usually outside is 0, inside is 100 and DMZ 50. In our case we will have outside with 0, inside with 100 and config with 100.

The default rules for TBFW are:
- Traffic from higher to lower trust levels is permitted.
- Traffic from lower to higher trust levels is denied, except if it is answering a corresponding traffic from higher to lower. This means, that if someone from inside asks for a webpage to a server situated on the outside, the request and the reply (the webpage) are allowed to pass automatically.
- Traffic between interfaces at the same trust level is denied, unless a special rule is added in the configuration.
- Interfaces can be grouped into SVI (switched virtual interfaces) an the trust level given on the SVI rather than on each interface. In this case traffic between interfaces of the same SVI is allowed.

The Windows XP IP address is 192.168.0.251 / 24 while ASA IP address in the CONFIG subnet is 192.168.0.1 / 24.

To run ASDM you need JAVA JRE which is already installed on the Windows XP virtual machine and you do not need to modify anything. My experience is that any JAVA JRE up to version 9 should be fine. I could not make it run under version 9. However, because the ASDM is older, it requires MD5 as hash (not as secured as SHA1 or SHA256). On a new machine, if you have problems connecting to the ASA via ASDM from Windows, you need to alter the following files:

On MacOS:
/Library/Internet\ Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/java.security
On Windows:
C:\Program Files\Java\jre_version\lib\security\java.security
C:\Program Files (x86)\Java\jre_version\lib\security\java.security

On Linux it should be a similar file to edit but I do not know the details as they differ from distribution to distribution.

Search for any apparition of MD5 and delete it from the list of restricted protocols. Simply put, anything containing MD5 as parameter should be erased. This has already been done in the Windows XP virtual machine so you do not have to do it.

On the Windows XP machine open Internet Explorer and type: https://192.168.0.1/admin. Accept to continue to the website. Click on Install ASDM Launcher. Let the launcher download and run it to install. It will create a shortcut on the desktop. You test ASDM on Windows XP. In Reality there is a version for MacOS, too.

On the Windows XP VM click the START button and go to Cisco ASDM-IDM Launcher. Put the IP address of ASA: 192.168.0.1, no username, password cisco. The first thing is a Wizard to create and export a self signed certificate. Play with it. Export it and import it into Windows XP. It should be easy. Do not forget to save the ASA configuration by clicking in ASDM the diskette on the bottom side of the display. That diskette appears whenever you change something in the configuration.

You can play with ASA and ASDM.

4. Updating ASA and ASDM to the latest version

We need to update the ASA machine to the latest firmware version and ASDM to the latest one. In the classic mode we need a TFTP server which was already installed in the Windows XP machine. However, let us try the ASDM way.

If you look at the parameters, you now run ASA version 9.1(5).21 and ASDM 7.4(3)

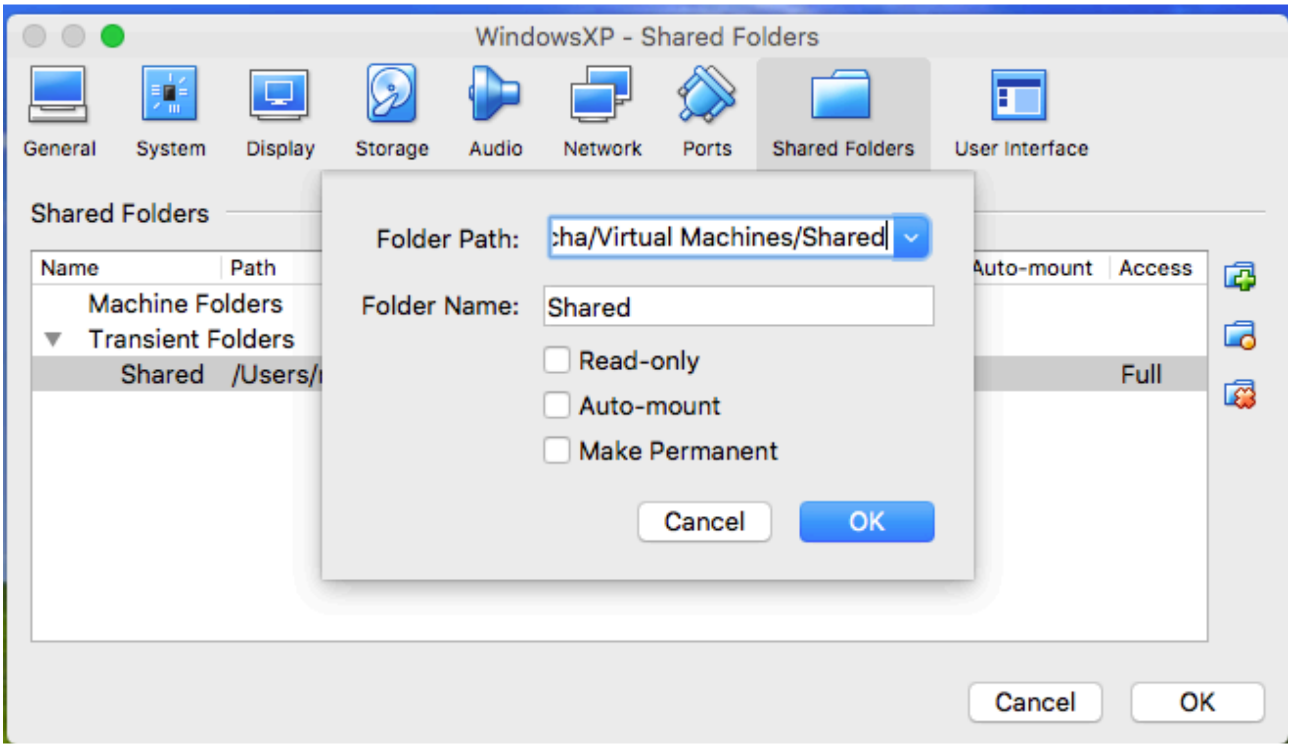
You need to download the following files on your computer:

asa924-24-k8.bin - this is the operating system

asdm-782.bin - this is the ASDM

You find them here: https://moucha.org/bissb-2017/asa-latest.zip or (because the download is around 60 MB) you cen receive them from your teacher.

Download the zip to your real computer and move it to the Windows XP. To do that there are 2 options: drag-and-drop from the real machine to the XP (may not always work) or Shared Folder. You find the Shared Folder setup on the VirtualBox, Machine, Settings, Shared Folder. Make a shared folder on your real machine using that menu (Figure 11):



Shared Folders

Name	Path	Auto-mount	Access
Machine Folders			
▼ Transient Folders			
Shared	/Users/		Full

Folder Path: :ha/Virtual Machines/Shared

Folder Name: Shared

□ Read-only

□ Auto-mount

□ Make Permanent

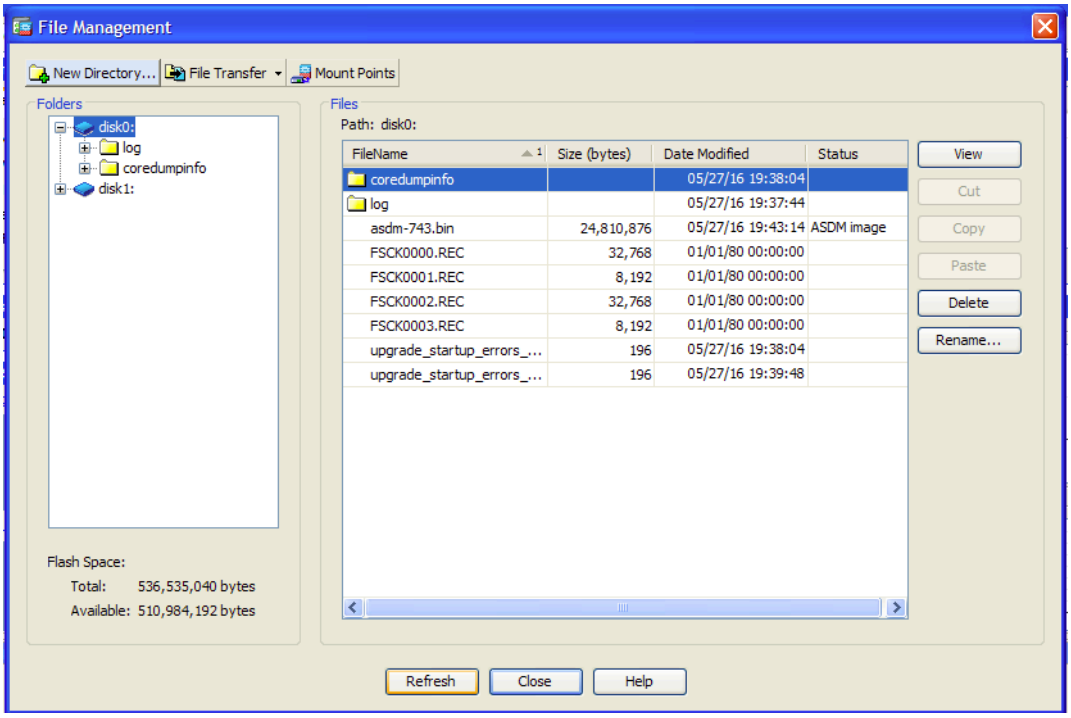
Figure 11 - creating a shared folder.

Put the downloaded file(s) into the shared folder on your real computer. You will access the shared folder from here:

On the XP VM, Desktop, open My Network Places. Click Entire Network, VirtualBox Shared Folders, \\Vboxsvr, \\VBOXSVR\Shared and inside you will see your shared files. Copy them to your Desktop on the XP VM.

Open the ASDM and connect to the ASA.

Go in the top menu (File, View, etc) on Tools and then open File Management. This will open (Figure 12):



Path: disk0:

FileName	Size (bytes)	Date Modified	Status
coredumpinfo		05/27/16 19:38:04	
log		05/27/16 19:37:44	
asdm-743.bin	24,810,876	05/27/16 19:43:14	ASDM image
FSCK0000.REC	32,768	01/01/80 00:00:00	
FSCK0001.REC	8,192	01/01/80 00:00:00	
FSCK0002.REC	32,768	01/01/80 00:00:00	
FSCK0003.REC	8,192	01/01/80 00:00:00	
upgrade_startup_errors_...	196	05/27/16 19:38:04	
upgrade_startup_errors_...	196	05/27/16 19:39:48	

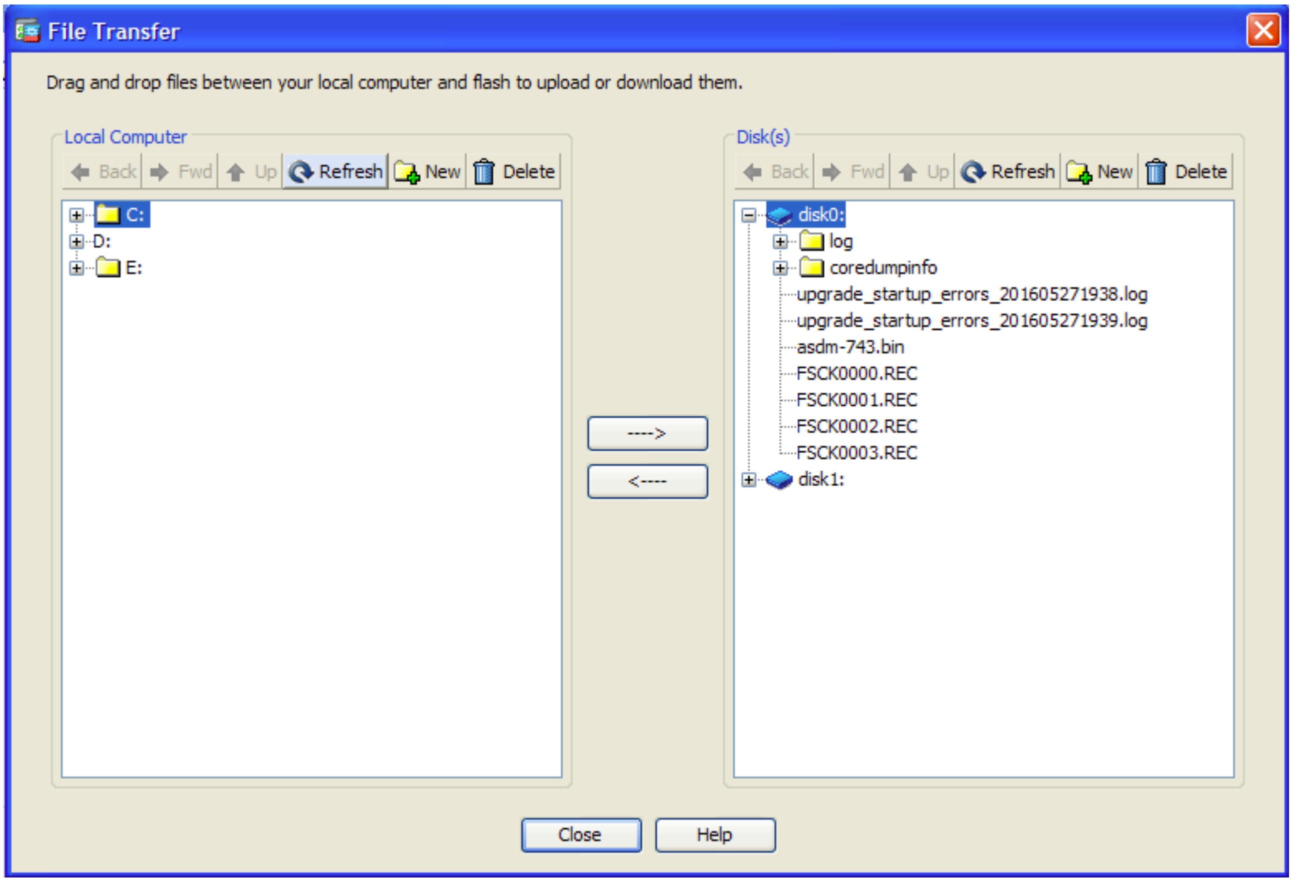
Flash Space:

Total: 536,535,040 bytes

Available: 510,984,192 bytes

Figure 12 - the File Manager

In the File Management click File Transfer and choose File Transfer Between Local PC and Flash, as in Figure 13:


File Transfer

Drag and drop files between your local computer and flash to upload or download them.

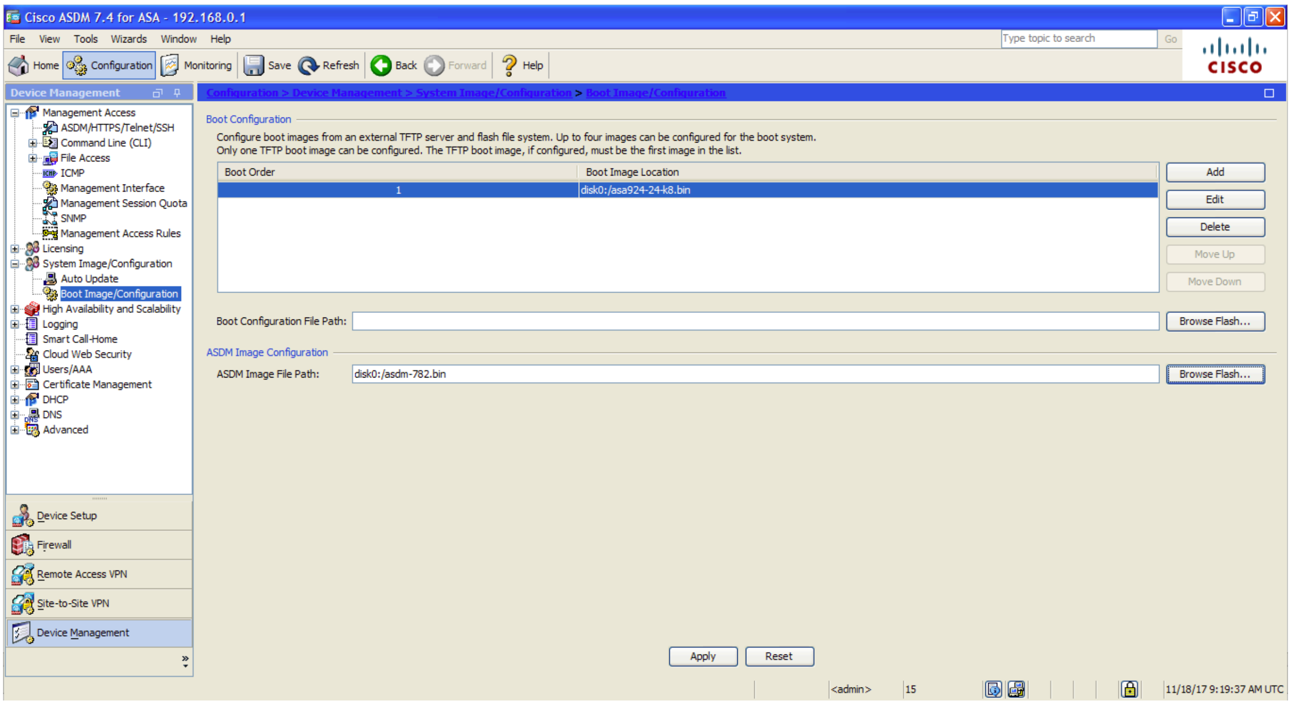
Figure 13 - transfer of files.

On the left-hand side go where you have the dowloaded latest firmware (either on desktop or on the shared folder, which, if you did not unmount it, will still be visible). On the right-hand side choose the flash of the ASA (usually disk0). You can verify it by opening the ASA command line and typing *show flash* at #. The files should be the same.

Copy the asa firmware and asdm to the flash by choosing each and clicking the arrow -> pointing from left to right. A progress bar should appear and you see the files copied. After each file you should see “File Upload Success”.

Close the file transfer and close the file management.

In the ASDM click Configuration (large button with some cogs on it). Go in the lefthand side menu and choose Device Management (down) and then System Image/Configuration (up). Figure 14:



Boot Configuration

Configure boot images from an external TFTP server and flash file system. Up to four images can be configured for the boot system. Only one TFTP boot image can be configured. The TFTP boot image, if configured, must be the first image in the list.

Boot Order	Boot Image Location
1	disk0:/asa924-24-k8.bin

Boot Configuration File Path:

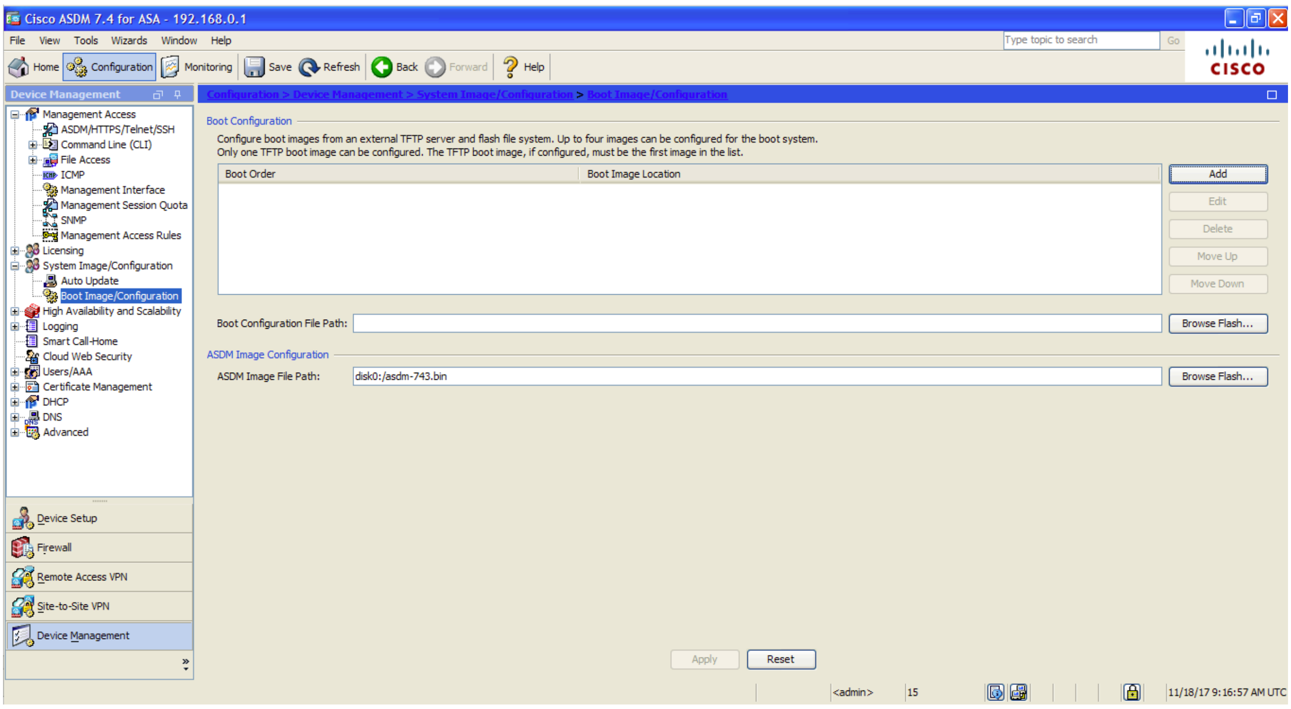
ASDM Image Configuration

ASDM Image File Path: disk0:/asdm-782.bin

Figure 14: System Configuration

Click Boot Order and Add from Flash Image -> Browse Flash and choose the asa924-24-k8.bin file which you uploaded. Click OK twice.

Then, on the field ASDM Image File Path click Browse Flash and select asdm-782.bin from the flash. The result has to be like in Figure 15:



Boot Configuration

Configure boot images from an external TFTP server and flash file system. Up to four images can be configured for the boot system. Only one TFTP boot image can be configured. The TFTP boot image, if configured, must be the first image in the list.

Boot Order	Boot Image Location

Boot Configuration File Path:

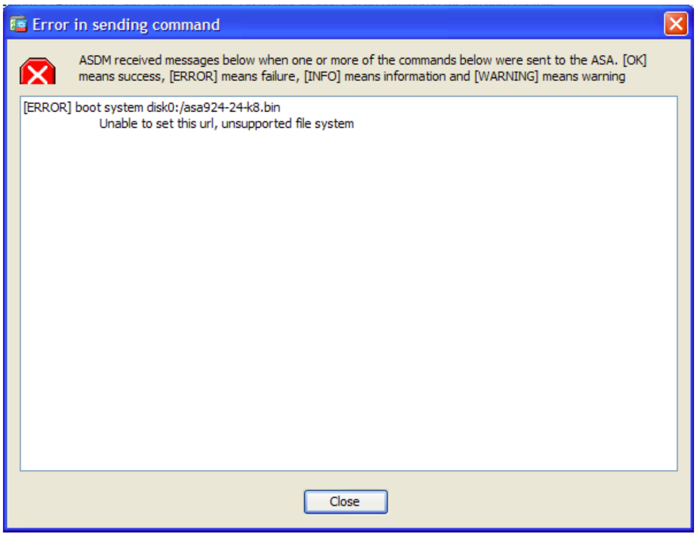
ASDM Image Configuration

ASDM Image File Path: disk0:/asdm-743.bin

Figure 15 - the new configuration.

DO NOT CLICK APPLY!!! UNFORTUNATELY ERROR!!!

This is how you would do it in the real world, but in the GNS3 I got an error (Figure 16):



ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning

```
[ERROR] boot system disk0:/asa924-24-k8.bin
        Unable to set this url, unsupported file system
```

Figure 16 - The error. ASDM went fine (OK) but not the operating system.

If you really want to run the latest and greatest firmware, follow the instructions here to hack a RAM disk and a Kernel image from the bin file I provided you: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/september/cisco-asa-series-part-two-static-analysis-and-datamining-of-cisco-asa-firmware/. This is however not mandatory for the subject SSB and I am not going to do this because of lack of time.

Revert all settings by reloading the ASA in command line (*reload*), by restarting GNS3. DO NOT SAVE THE CONFIGURATION if prompted.

If you did something wrong, do not worry. At any time you can replace your broken project with the clean one which I gave.

5. The First “Real” Network

For this we are going to put two routers and simulate the INSIDE and OUTSIDE zones.

Put two routers 3725 firmware and connect them to the ASA. I connected them like this:

R1 Fast Ethernet 0/0 to ASA Ethernet 0 (on ASA even if the ports are called “Ethernet” they are in fact Gigabit). R2 Fast Ethernet 0/1 to ASA Ethernet 1. (Figure 17)

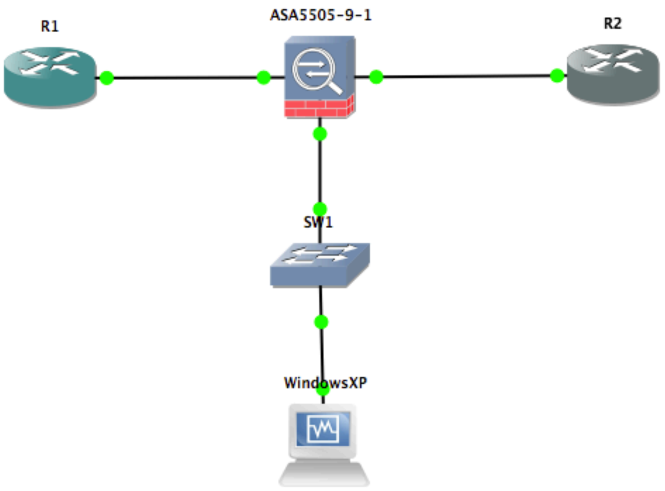


Figure 17 - The new topology.

Let us configure the routers.

Using the Lab Manual 1 configure on R1 the IP address 2.0.0.2 and turn the interface on. This router will play the role of INSIDE. Put a default gateway to 2.0.0.1 (*ip route 0.0.0.0 0.0.0.0 2.0.0.1).* Use the first manual for guidance on the commands.

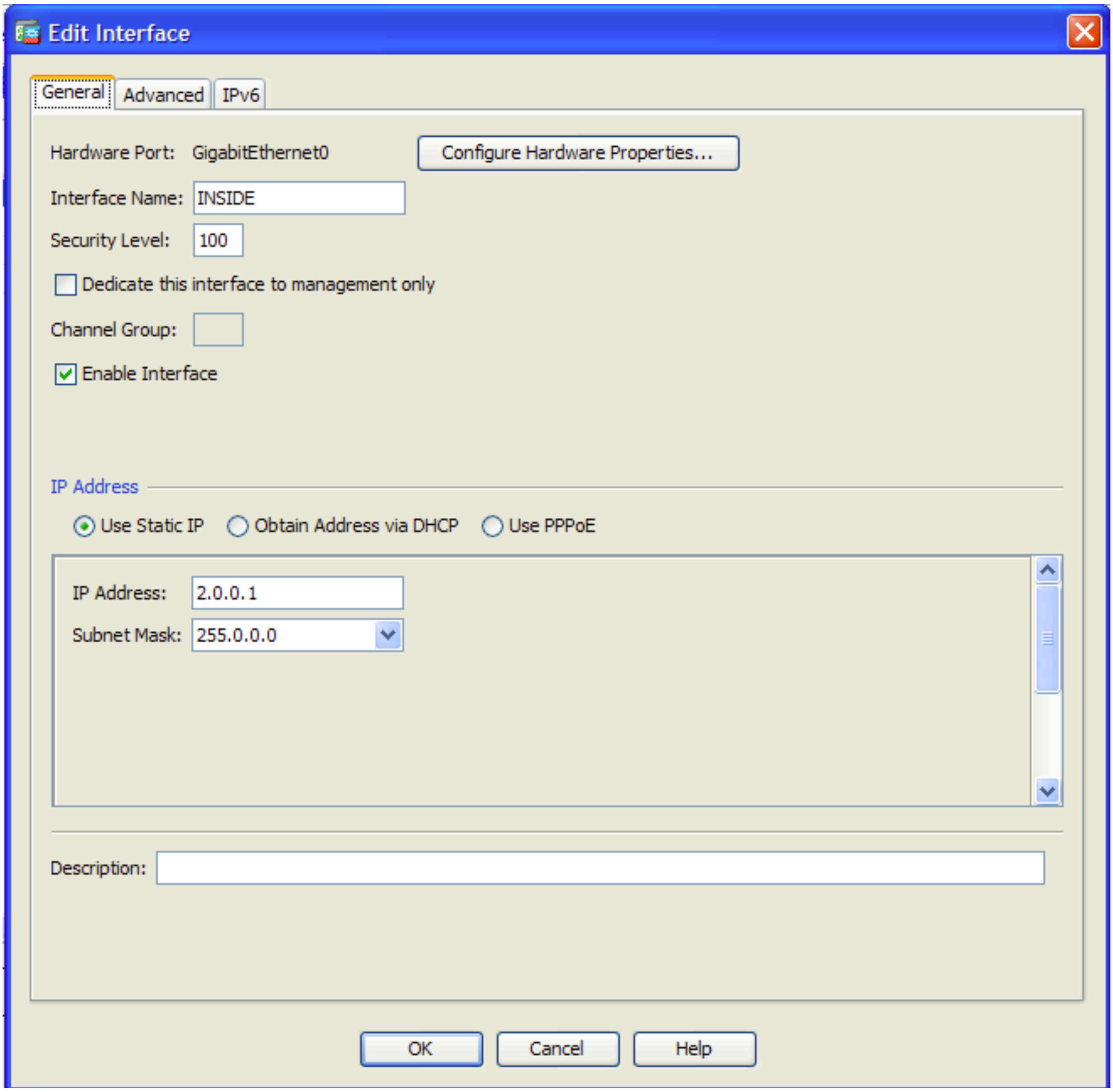
Configure on R2 the ip address 1.0.0.2 and turn the interface on. This will play the role of OUTSIDE. Add a default gateway to 1.0.0.1.

Configure a TELNET server on R1 and R2. They are explained in manual 1, chapter 7.

What remains is to configure the ASA 5505. Open ASDM and connect to the ASA.

Go on Configuration (big button with cogs) In the down part click Device Setup and choose from the menu Interface Settings and then Interfaces.

Double-Click Gigabit 0. Put the security name INSIDE, the trust (security) level 100 and set the IP address to 2.0.0.1. Check the checkbox Enable Interface. Read the warning and close it. (Figure 18).


Edit Interface

General | Advanced | IPv6

Hardware Port: GigabitEthernet0

Interface Name: INSIDE

Security Level: 100

□ Dedicate this interface to management only

Channel Group:

☑ Enable Interface

IP Address

● Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE

IP Address: 2.0.0.1

Subnet Mask: 255.0.0.0

Description:

Figure 18 - The setup of the interface Gigabit 0.

Then, double-Click Gigabit 1. Put the security name OUTSIDE, the trust (security) level 0 and set the IP address to 1.0.0.1. Check the checkbox Enable Interface. Read the warning and close it.

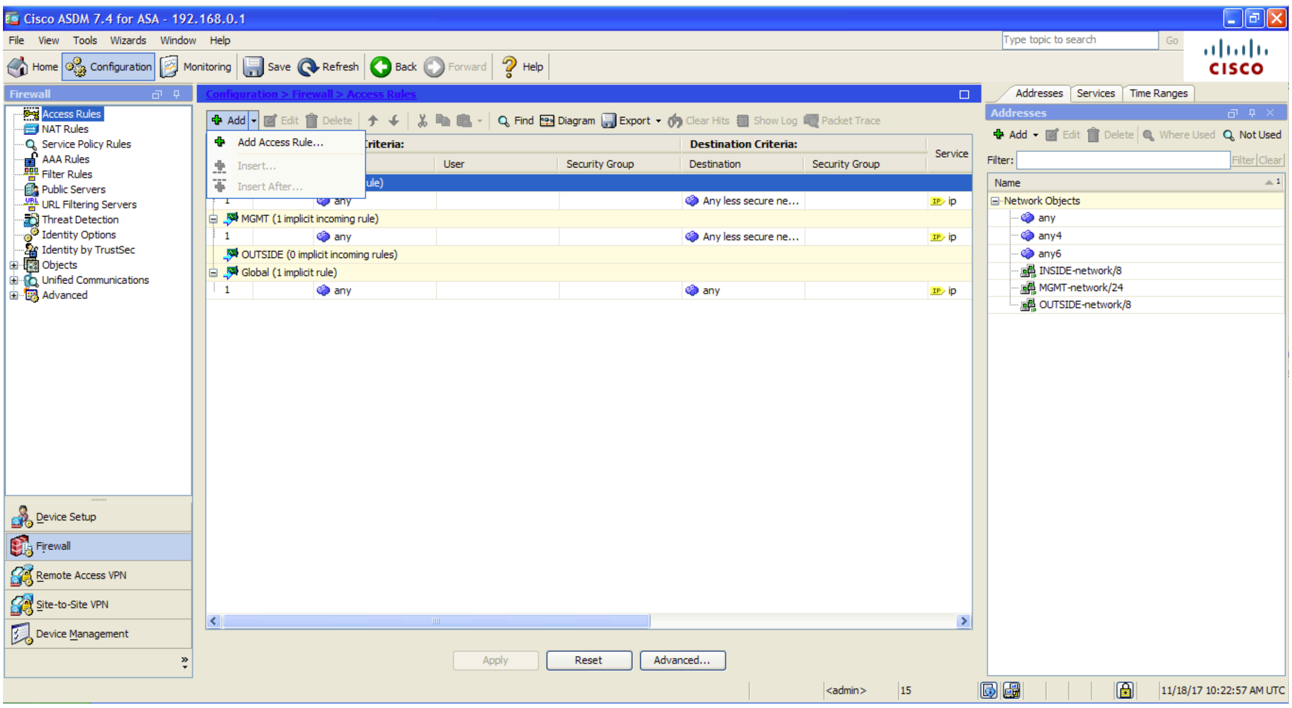
Click APPLY. Save the configuration using the diskette.

Test ping connectivity and TELNET between R1 and R2 (both directions).

Result 1: TELNET works only from INSIDE going OUTSIDE but not backwards (due to difference in trust levels - see the rules in Chapter 4).

Result 2: ping does not work in any direction? Why? Because it is filtered completely by the firewall. Let us permit it.

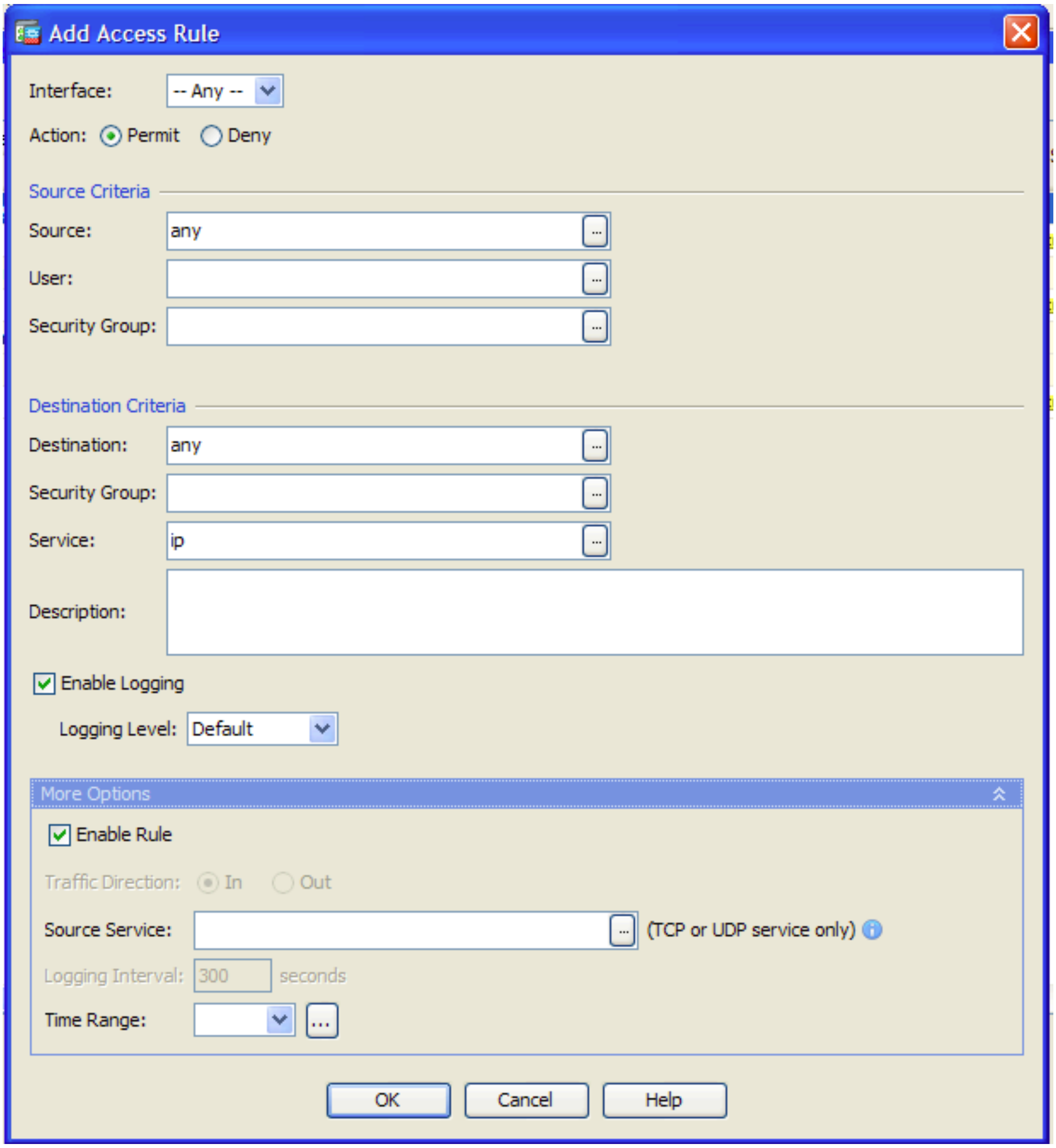
Go into ASDM and click Configure (the button with the cogs). Click in the lefthand side down on Firewall. We shall add an ACL rule (Figure 19).



	riteria:			Destination Criteria:		Service
		User	Security Group	Destination	Security Group	
ule)						
1	any			Any less secure ne...		ip
MGMT (1 implicit incoming rule)						
1	any			Any less secure ne...		ip
OUTSIDE (0 implicit incoming rules)						
Global (1 implicit rule)						
1	any			any		ip

Figure 19 - the firewall menu.

Click Add, choose any interface, any source, any destination, enable rule but choose protocol icmp. Figure 20:



Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: any

Security Group:

Service: ip

Description:

☑ Enable Logging

Logging Level: Default

More Options

☑ Enable Rule

Traffic Direction: ● In ○ Out

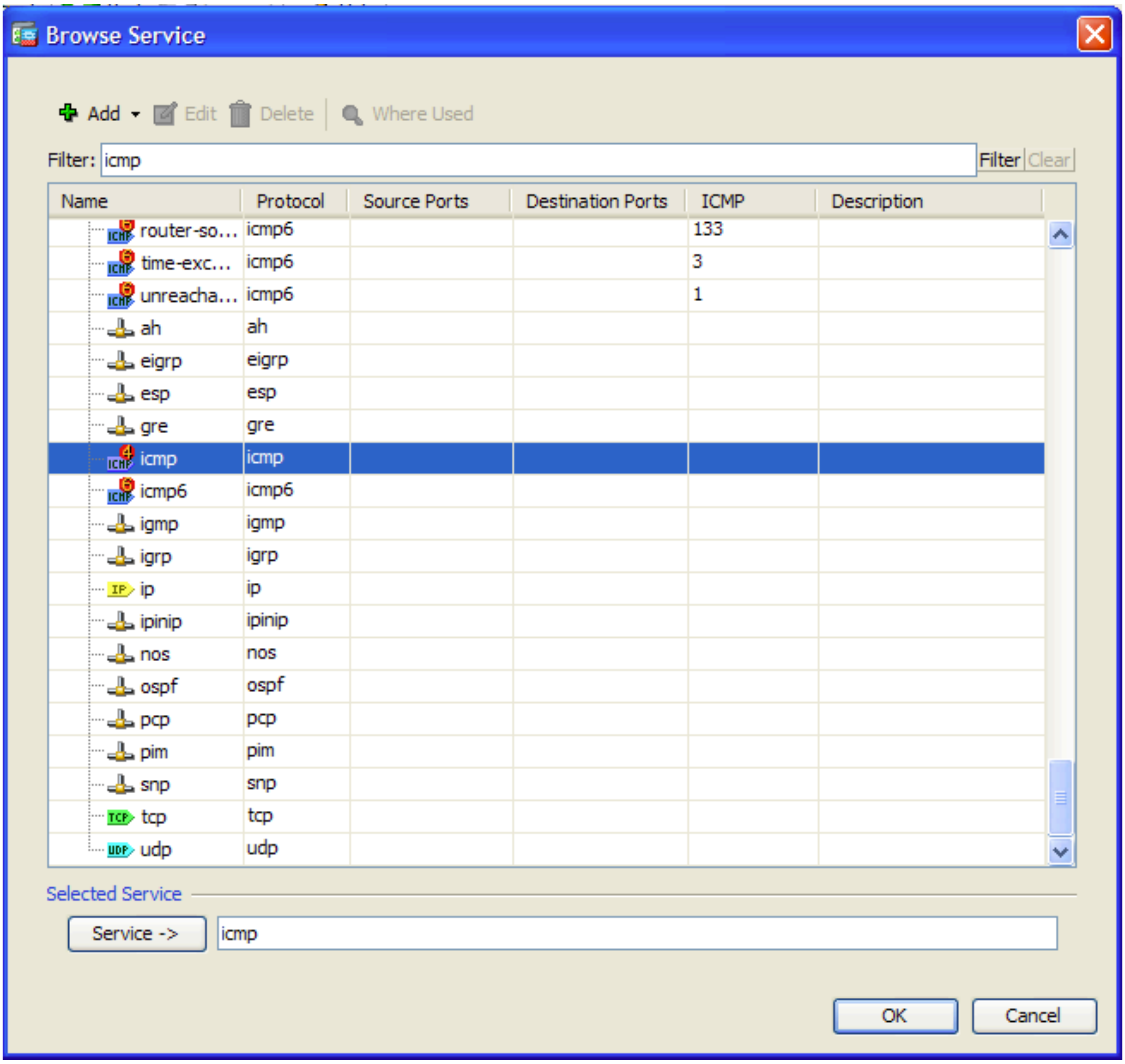
Source Service: (TCP or UDP service only)

Logging Interval: 300 seconds

Time Range:

Figure 20 - The addition of a new ACL rule.

The icmp protocol should be selected (Figure 21):



Filter: icmp

Name	Protocol	Source Ports	Destination Ports	ICMP	Description
router-so…	icmp6			133	
time-exc…	icmp6			3	
unreacha…	icmp6			1	
ah	ah				
eigrp	eigrp				
esp	esp				
gre	gre				
icmp	icmp				
icmp6	icmp6				
igmp	igmp				
igrp	igrp				
ip	ip				
ipinip	ipinip				
nos	nos				
ospf	ospf				
pcp	pcp				
pim	pim				
snp	snp				
tcp	tcp				
udp	udp				

Service -> icmp

Figure 21 - The selection of icmp.

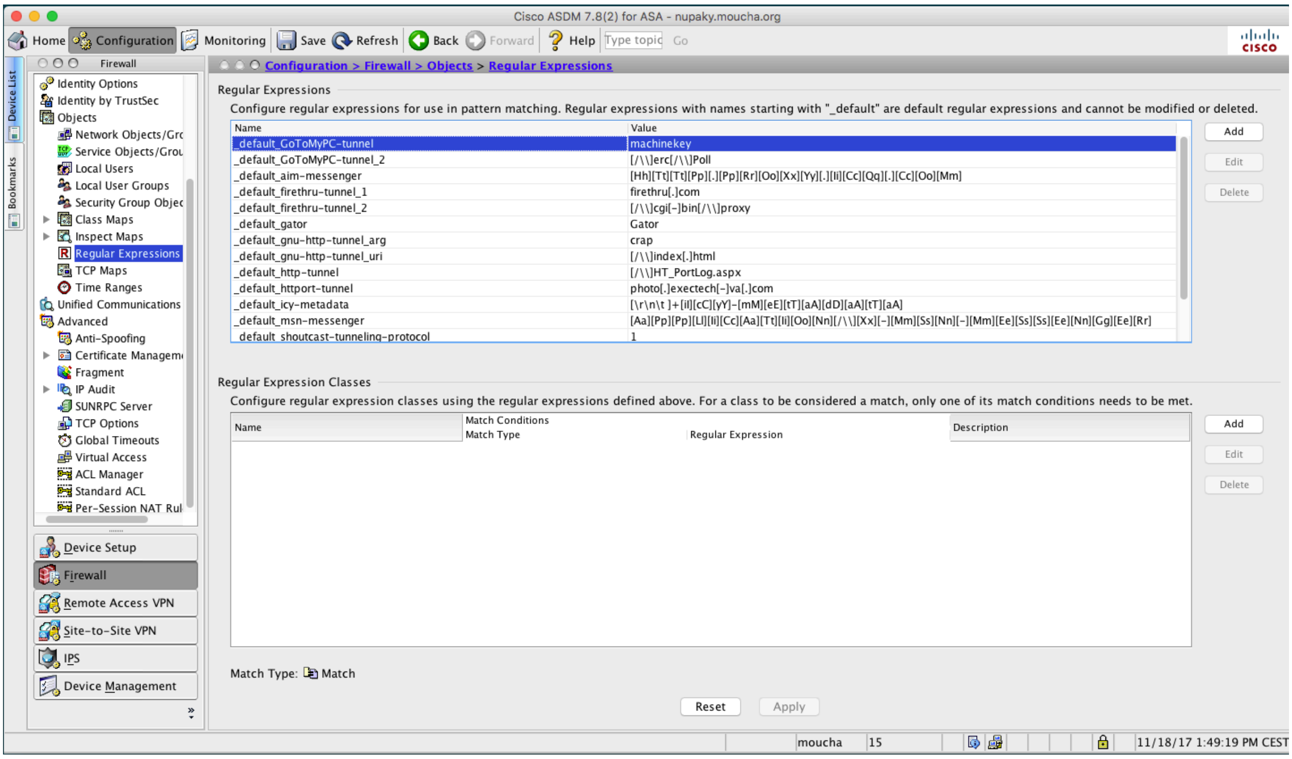
Click OK, OK, Apply and save.

Ping should now work in any direction.

6. Extra - If you want

Try to configure a username for ASA and password. Google it.

Also, you can see in the configuration of the Firewall a lot of settings (Figure 22). These are very complex but look: regular expressions. You can filter traffic in a very fine way. For example, if you have in a webpage fields to put the credit card number but the connection is not https, ASA will filter the fields in relation with the credit card so thus a non-technical user cannot fill them in by mistake. And you have a screenshot from the ASDM on MacOS.



Regular Expressions

Configure regular expressions for use in pattern matching. Regular expressions with names starting with "_default" are default regular expressions and cannot be modified or deleted.

Name	Value
_default_GoToMyPC-tunnel	machinekey
_default_GoToMyPC-tunnel_2	[/\\]erc[/\\]Poll
_default_aim-messenger	[Hh][Tt][Tt][Pp][.][Pp][Rr][Oo][Xx][Yy][.][Ii][Cc][Qq][.][Cc][Oo][Mm]
_default_firethru-tunnel_1	firethru[.]com
_default_firethru-tunnel_2	[/\\]cgi[-]bin[/\\]proxy
_default_gator	Gator
_default_gnu-http-tunnel_arg	crap
_default_gnu-http-tunnel_uri	[/\\]index[.]html
_default_http-tunnel	[/\\]HT_PortLog.aspx
_default_httport-tunnel	photo[.]exectech[-]va[.]com
_default_icy-metadata	[\r\n\t]+[iI][cC][yY]-[mM][eE][tT][aA][dD][aA][tT][aA]
_default_msn-messenger	[Aa][Pp][Pp][Ll][Ii][Cc][Aa][Tt][Ii][Oo][Nn][/\\][Xx][-][Mm][Ss][Nn][-][Mm][Ee][Ss][Ss][Ee][Nn][Gg][Ee][Rr]
_default_shoutcast-tunneling-protocol	1

Regular Expression Classes

Configure regular expression classes using the regular expressions defined above. For a class to be considered a match, only one of its match conditions needs to be met.

Name	Match Conditions Match Type	Regular Expression	Description

Match Type: Match

Figure 22 - Extremely detailed settings for filtering and in-depth packet inspection.

You have now a fully working ASA lab.