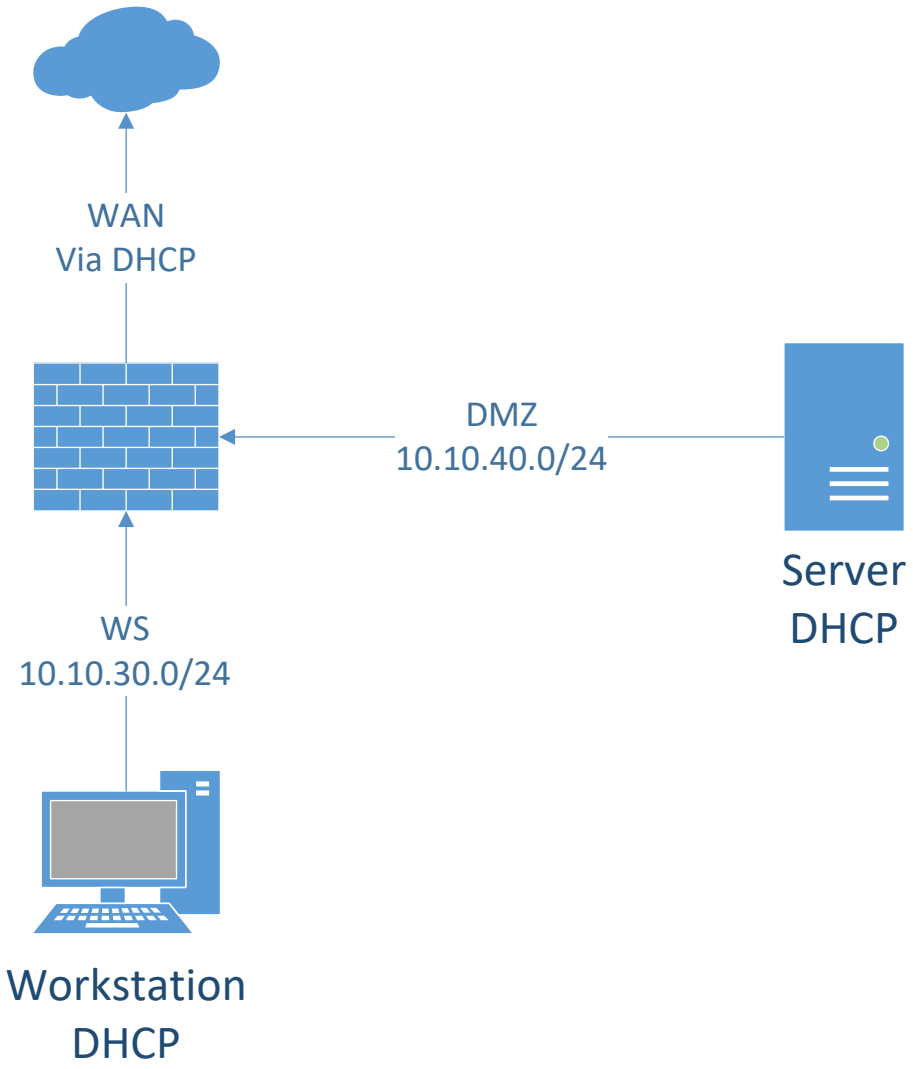
Lab6 – Paloalto basics

Document your commands or take screenshots. Answer questions in english or finnish.

Both Ubuntu credentials: Student/root-66

Paloalto: admin/admin

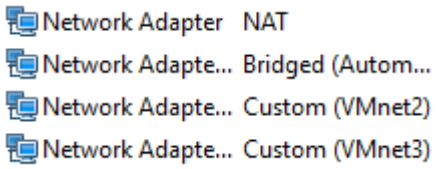
The labs use the following topology (Workstation will be Ubuntu Desktop):



- **Install Paloalto (1p)**

Retrieve the pre-installed VM images for Paloalto, Ubuntu Workstation and the Ubuntu server from \\ghost.labranet.jamk.fi\virtuaalikoneet\TTKS\VMware . Import them to VMware. Set interfaces as following:

Paloalto:



Ubuntu Desktop: Custom (VMnet2)

Ubuntu Server: Custom(VMnet3)

Next, we need to change which virtualDevices VMware uses for interfaces.

If you don't remember/know where you imported virtual machines, select virtual machines, go to options tab, and there you should be able to find Working directory.

Close VMware workstation and use explorer to navigatfiree where you imported virtual machines. There should be file like this:

Open it with notepad, find lines where it says ethernetX.virtualDev = "e1000" (Where X is any number, depends on how many virtual network adapters you have on VM), and change e1000 to vmxnet3. Maybe the easiest way is to Find and Replace e1000 to vmxnet3.

So for every interfaces you should change this:

```
ethernet0.virtualDev = "e1000"
```

to this:

```
ethernet0.virtualDev = "vmxnet3"
```

Save files and then open VMware again.

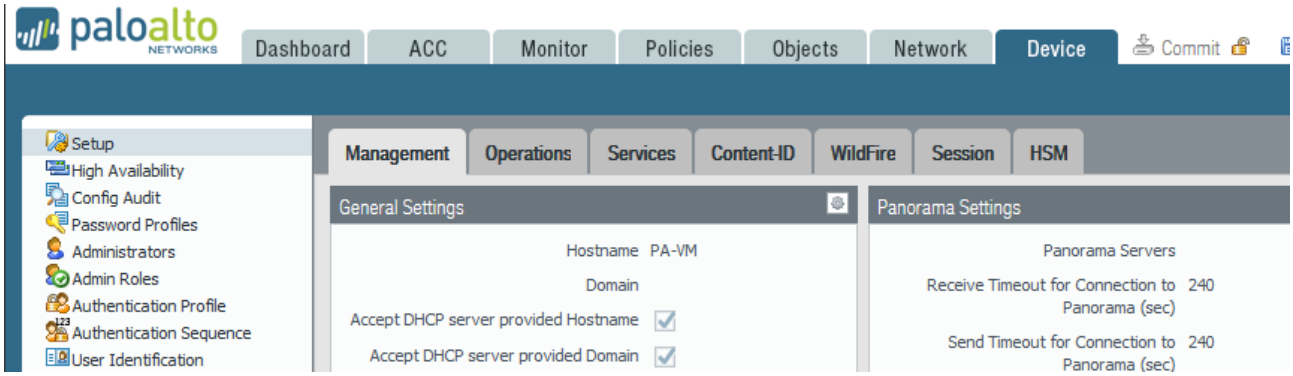
Next, boot up Paloalto, for login use admin/admin. It might take while before you actually can log in…

Then we need to figure out what ip address paloalto uses, type:

show interface all

and check Ip address for Ethernet1/1 .

Now we should be able to connect that ip address with host machine. Use firefox & Use HTTPS!!!!

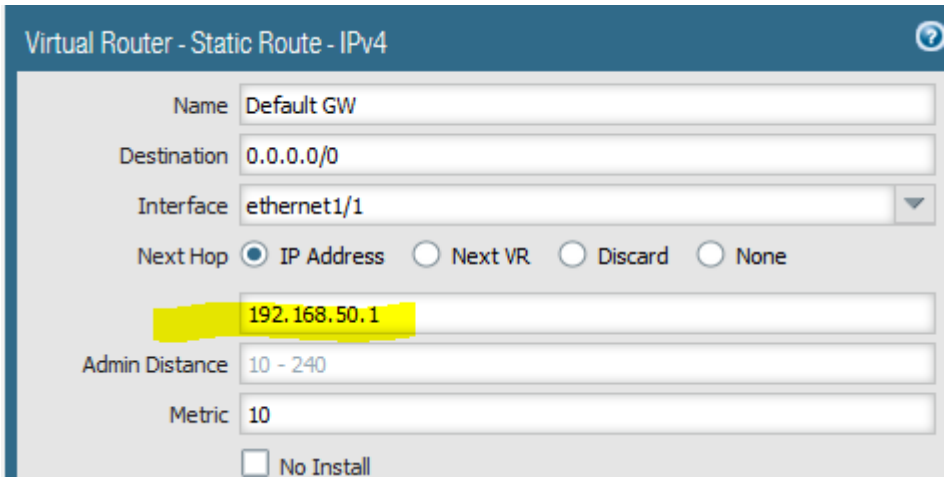


Toimii!!

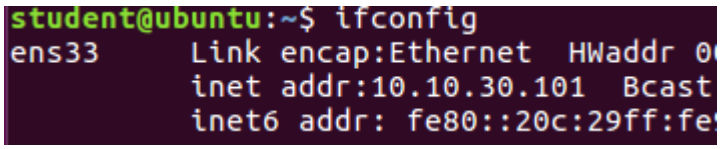
Ok, you get warning that connection isn't secure, add exception.

Login to paloalto from browser, then choose Network tab and Virtual Routers from there.

Select default, static routes, edit default gateway. Change next hop address to same that default gateway on your desktop.



Boot up the Ubuntu desktop (credentials are **student/root-66**) and check that it gets IP address from the Paloalto. If not, sudo ifdown ens33 then sudo ifup ens33.



When you get IP address, try accessing going to www.iltalehti.fi with a browser in the Ubuntu.

Do same with Ubuntu server, there isn't browser, but try wget iltasanomat.fi

```
student@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:3b:e2
          inet addr:10.10.40.101  Bcast:10.10.40.255
          inet6 addr: fe80::20c:29ff:fe3b:e2cb/64 Sc
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:16 errors:0 dropped:0 overruns:
          TX packets:35 errors:0 dropped:0 overruns:
          collisions:0 txqueuelen:1000
```

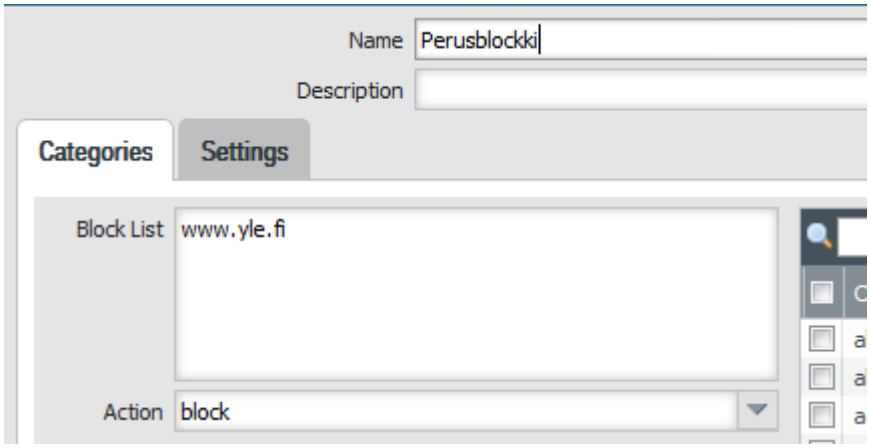
```
Connecting to www.is.fi (www.is.fi)|52.222.171.64|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 607828 (594K) [text/html]
Saving to: 'index.html.1'

index.html.1            100%[=====================================>] 593.58K  39.4KB/s

2017-03-22 11:26:06 (9.23 KB/s) - 'index.html.1' saved [607828/607828]

student@ubuntu:~$ _
```

- **License + URL FILTERING (1p)**

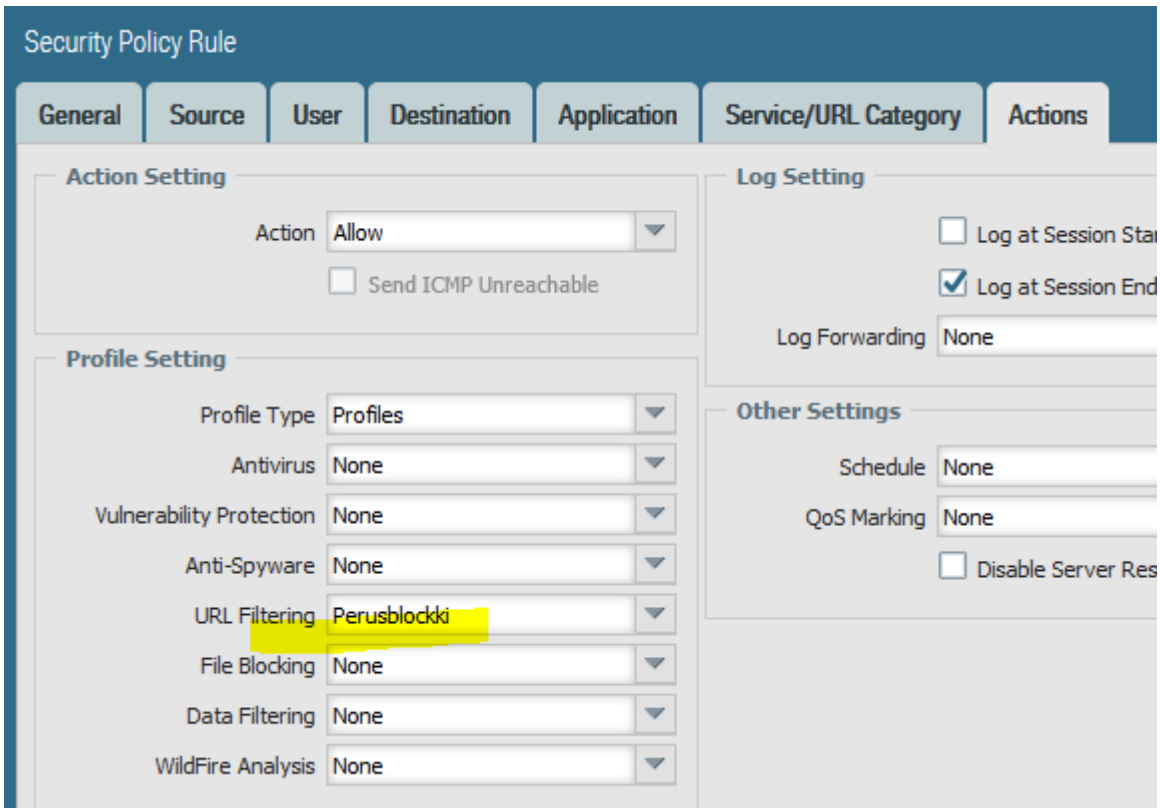
Go to Devices, Licenses, Activate feature using authorization code. Use license code: I9418680

Activation will reboot paloalto, So you may need to check which ip-address it did get this time…

Next try to figure out how to do url filtering, we want to block yle.fi.



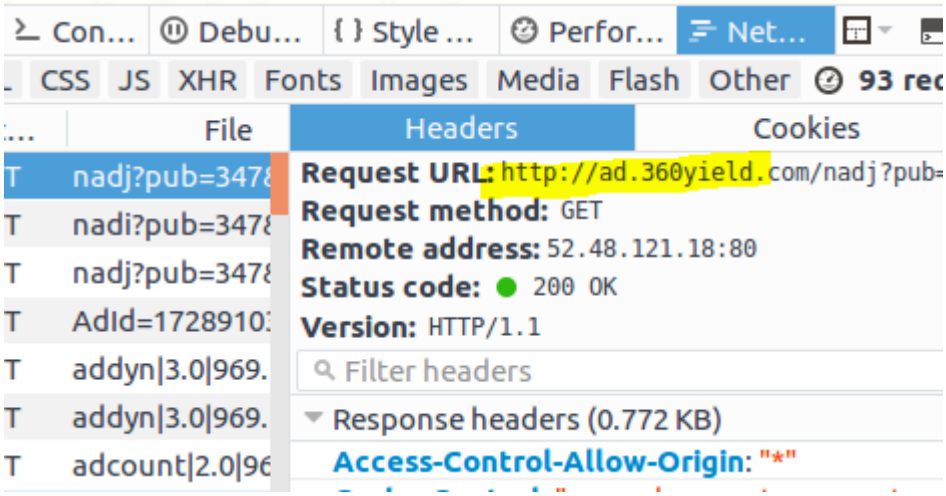
Lets block yle.fi

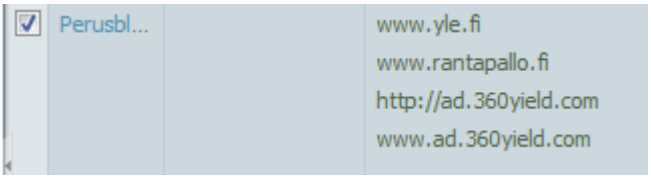


Try to block advertisements too on site you wish.

It is good to know that you can't block https sites or advertisements without configuring decryption, so try to find site where advertisements are http.

Block adds from source:



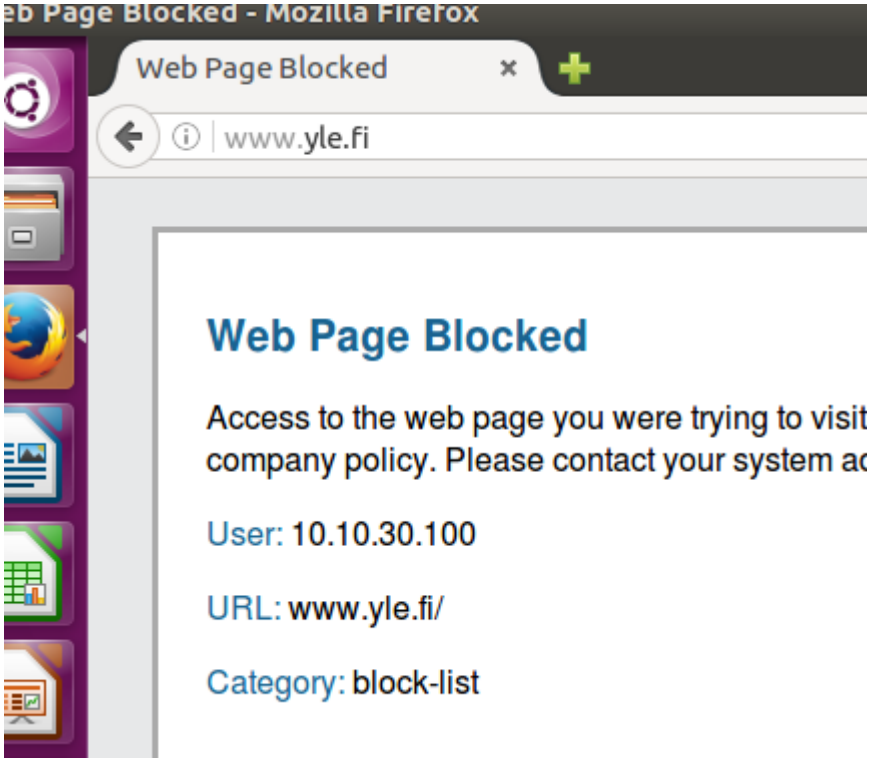


Remember to take screenshot form blocked site & Url filtering monitor…

Add request blocking was succesfull

	Receive Time	Category	URL	From Zone	To Zone	Source
	03/22 10:13:30	block-list	ad.360yield.com/nadj?...	WS	WAN	10.10.30.100
	03/22 10:13:30	block-list	ad.360yield.com/nadj?...	WS	WAN	10.10.30.100
	03/22 10:13:26	block-list	ad.360yield.com/nadj?...	WS	WAN	10.10.30.100
	03/22 10:13:23	block-list	ad.360yield.com/nadj?...	WS	WAN	10.10.30.100
	03/22 10:13:23	block-list	ad.360yield.com/nadj?...	WS	WAN	10.10.30.100
	03/22 10:04:28	block-list	www.yle.fi/favicon.ico	WS	WAN	10.10.30.100
	03/22 10:04:28	block-list	www.yle.fi/favicon.ico	WS	WAN	10.10.30.100
	03/22 10:04:26	block-list	www.yle.fi/	WS	WAN	10.10.30.100

YLE blocked:



- **Firewall Rules (1p)**

Ubuntu server has Apache running on it, make rule which allows you to browse from Ubuntu Desktop to it. So you need to make new security policy, from WS to DMZ, where you allow web-browsing

Rule to allow http:

	Name	Tags	Type	Source				Destination		Application	Service
				Zone	Address	User	HIP Profile	Zone	Address		
1	Default-allow-any	none	universal	DMZ WS	any	any	any	WAN	any	any	application-d..
2	HTTP	none	universal	WS	any	any	any	DMZ	any	any	service-http
3	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
4	interzone-default	none	interzone	any	any	any	any	any	any	any	any

Ubuntu server has also ssh-server running on it, make rule so you can take ssh connection from Desktop to it..

First trying without the rule and then with the rule where is allowed ssh on 22:

```
student@ubuntu:~$ ssh student@10.10.40.101
ssh: connect to host 10.10.40.101 port 22: Connection timed out
student@ubuntu:~$ ssh student@10.10.40.101
The authenticity of host '10.10.40.101 (10.10.40.101)' can't be establish
ECDSA key fingerprint is SHA256:3wLG6UpH0Mc1RFGqCYhNU8/C2ItGqrLaQ+Wo6vXVy
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.40.101' (ECDSA) to the list of known ho
student@10.10.40.101's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Wed Mar 22 11:19:42 2017
student@ubuntu:~$
```

SSH RULE:

- **WWW NAT (1p)**

In this lab we configure a port forward -based NAT. Incoming connection to port 80 from the WAN will be forwarded to the webserver.

First you need to create webserver-private and webserver-public objects, so go to Objects -> addresses

Add those two objects, for private set address to your server address.

For public set address to be same which one you have on ethernet1/1 (Click dynamic to see it)

	Name	Location	Type	Address
☐	webserver-private		IP Netmask	10.10.40.101
☑	webserver-public		IP Netmask	192.168.50.11

To get NAT working you need to do 2 things:

NAT rule and security rule

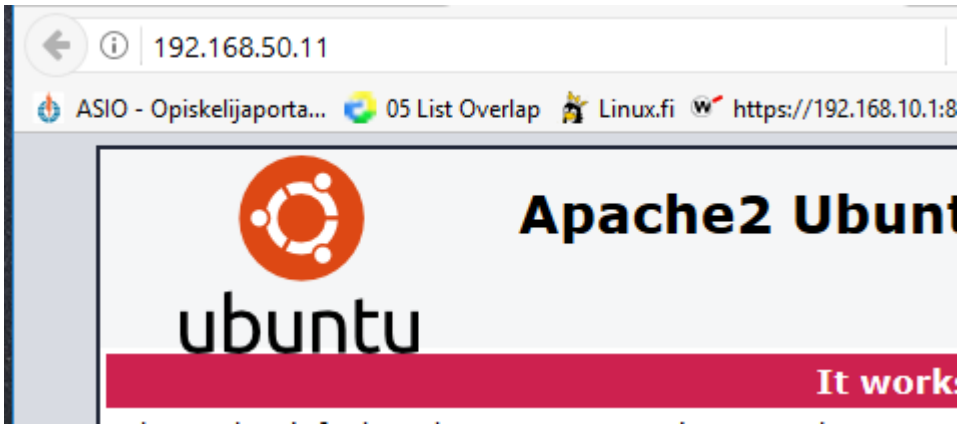
For NAT Source Zone WAN to Dest zone wan,any source, destination address is webserver-public service service-http

NAT RULE PORT FORWARD

- destination translation address: webserver-private port 80

Security rule: from zone WAN to destination zone dmz and destination address webservers-public application web-browsing service any.

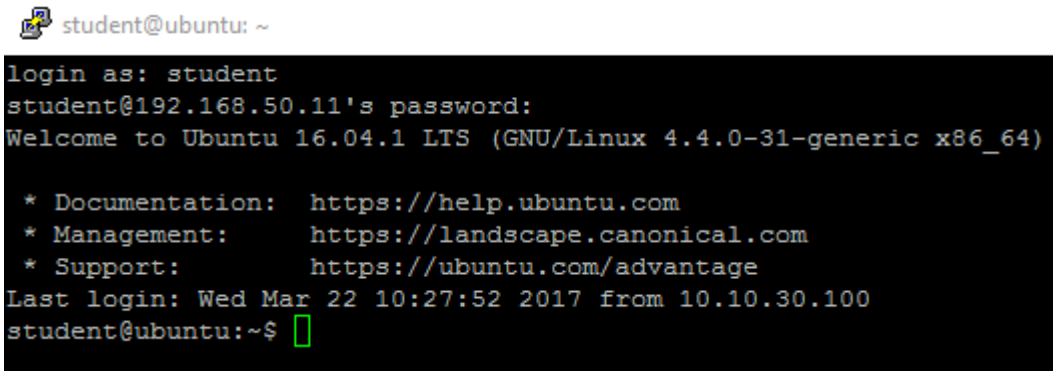
Policy WWW



- **SSH NAT (1p)**

Almost same as how you configured www NAT, now we just want do it for SSH, prove that you did get it working by taking ssh connection from windows host with putty ☺

SSH WORKS:



NAT RULE FOR SSH

POLICY TO SSH : WAN TO DMZ