## IP Forwarding with Mikrotik (https://mikrotik.com/download)

**LAB Overview**

This lab will show you how to use IP Forwarding with NVA based on Mikrotik.

Mikrotik is not officially available and supported on Azure but it works.

You can also use Citrix ADC: Load Balancer, SSL VPN, WAF & SSO, which have a Free Tier and many more images from Marketplace. (<https://azuremarketplace.microsoft.com/en/marketplace/apps/citrix.netscalervpx-120?tab=Overview>)

In this lab you will use following resources.

If you already have some of them, you don’t need to create them again.

1) VM – name: routerOS

2) VM – name: ubuntu01, which will sit in solution subnet.

3) VNET – name: vnet01-mng (this name will be used in this lab). In this VNET we will put routerVM based on Mikrotik and the VM, from which we will test the solution

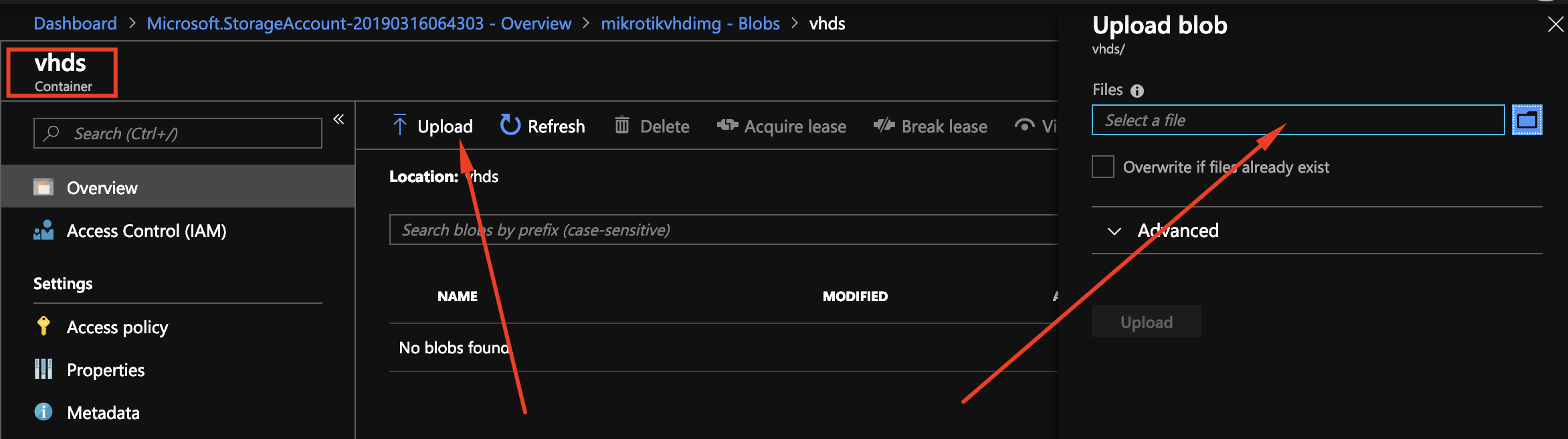
4) SUBNETS – you need three subnets. Two for MikrotikVM as it will use two NICs (**fesubnet** for external traffic and **bckendsubnet** for backend traffic), and one for the VM, from which we will test the solution (**solutionsubnet**)

**Task 1: Upload the Mikrotik VHD image**

Download Mikrotik VHD image from the link: <https://mikrotik.com/download> (it will be VHDX image but it is easy to convert it to VHD using command <https://www.abort-retry-fail.com/2018/09/29/how-to-convert-a-virtual-hard-disk-file-vhdx-to-vhd/>)

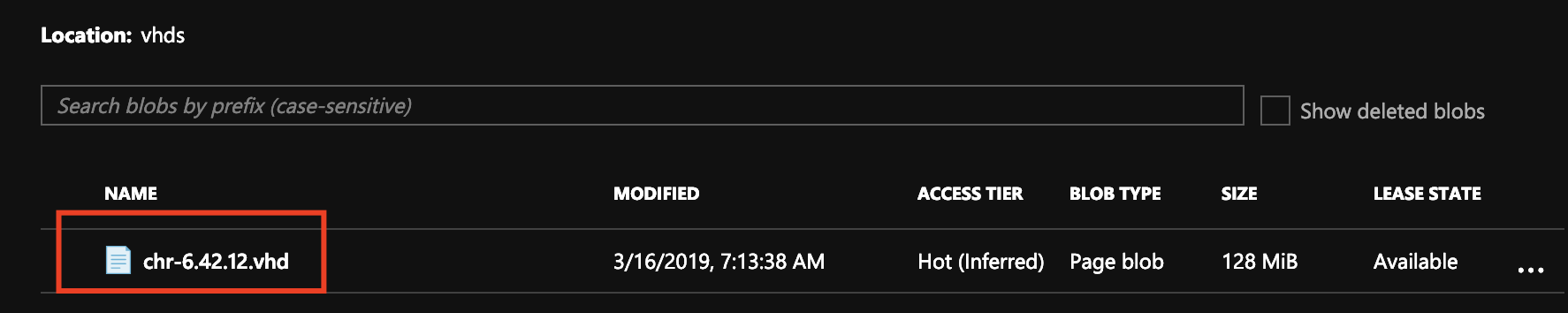
)

1. Sign in the Azure portal at [https://portal.azure.com](https://portal.azure.com/)
2. Create a simple Storage Account or reuse one you have in the same region where you want to create the Mikrotik VM.
3. Go to Storage Account and create the container, name it **vhds**.
4. Upload the VHD file you have downloaded in the step 1 to this container.



1. After you upload the file, please make sure you make not of the name of the vhd file.

In my case this is:



1. Once the file will be uploaded, open the PowerShell console, which we will need to create our VM.
2. Please download the script, which will help create the VM:

<https://raw.githubusercontent.com/mifurm/networkinginazure/master/createroutervm.ps1>

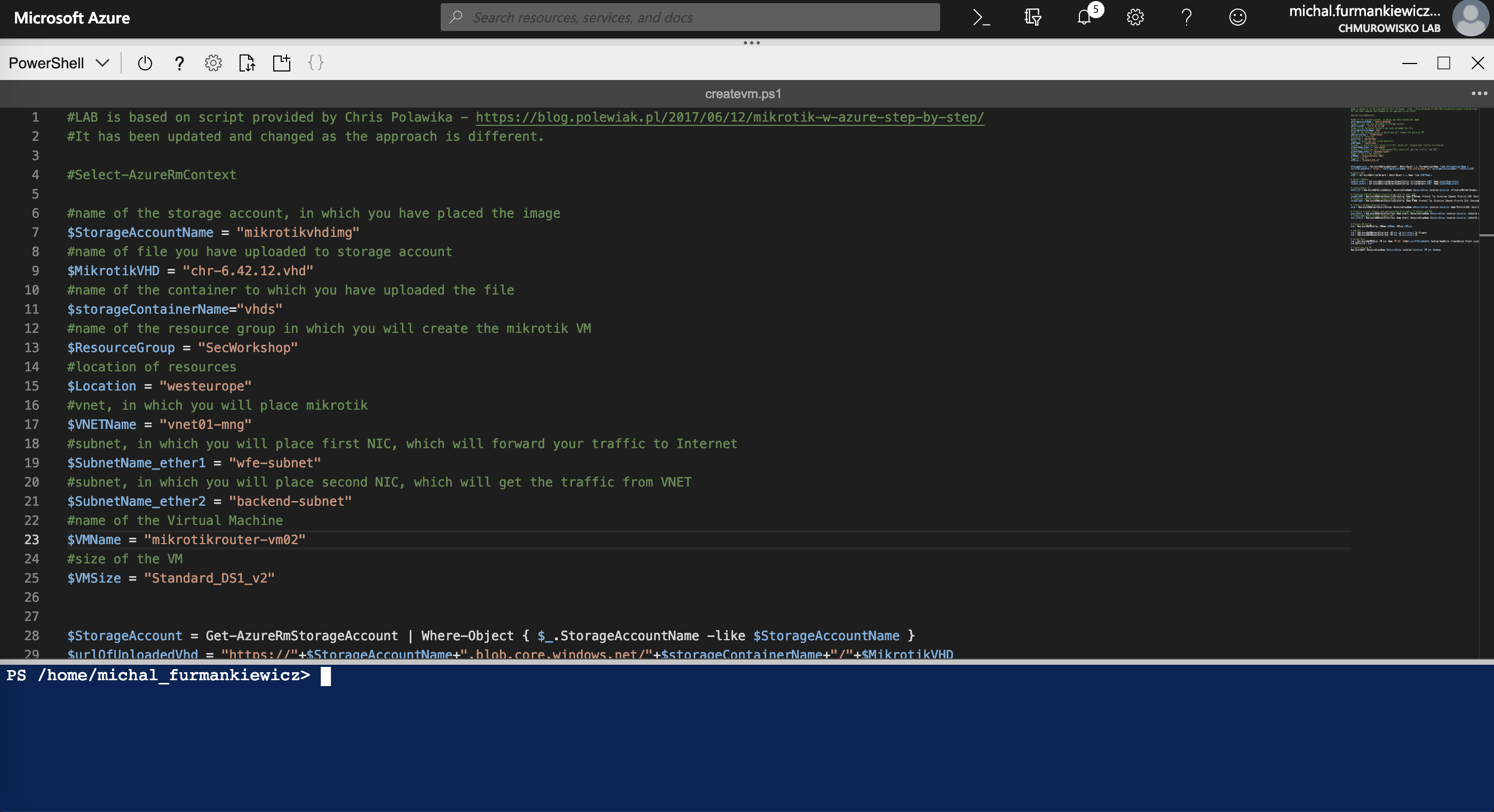
We will create the VM image in another Task.

**Task 2: Create Mikrotik VM**

1. Sign in the Azure portal at https://portal.azure.com
2. Please open Windows PowerShell ISE and login into your subscription
3. You can use PowerShell Console inside portal. I will use exactly this one for the sake of this lab.

You can also run an editor VS Code, by typing code into PowerShell Console.

It will be easier for you to modify and update files.

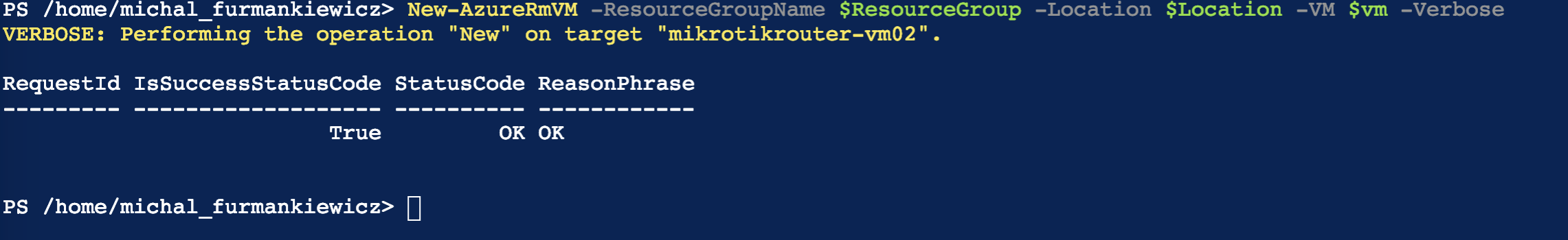


1. Please update the lines with all variables to reflect your environment.

Make sure all the lines reflect all your local settings. Before every line you will find a comment to help you put the right data there.

1. #name of the storage account, in which you have placed the image
2. $StorageAccountName = "mikrotikvhdimg"
3. #name of file you have uploaded to storage account
4. $MikrotikVHD = "chr-6.42.12.vhd"
5. #name of the container to which you have uploaded the file
6. $storageContainerName="vhds"
7. #name of the resource group in which you will create the mikrotik VM
8. $ResourceGroup = "SecWorkshop"
9. #location of resources
10. $Location = "westeurope"
11. #vnet, in which you will place mikrotik
12. $VNETName = "vnet01-mng"
13. #subnet, in which you will place first NIC, which will forward your traffic to Internet
14. $SubnetName\_ether1 = "wfe-subnet"
15. #subnet, in which you will place second NIC, which will get the traffic from VNET
16. $SubnetName\_ether2 = "backend-subnet"
17. #name of the Virtual Machine
18. $VMName = "mikrotikrouter-vm02"
19. #size of the VM
20. $VMSize = "Standard\_DS1\_v2"

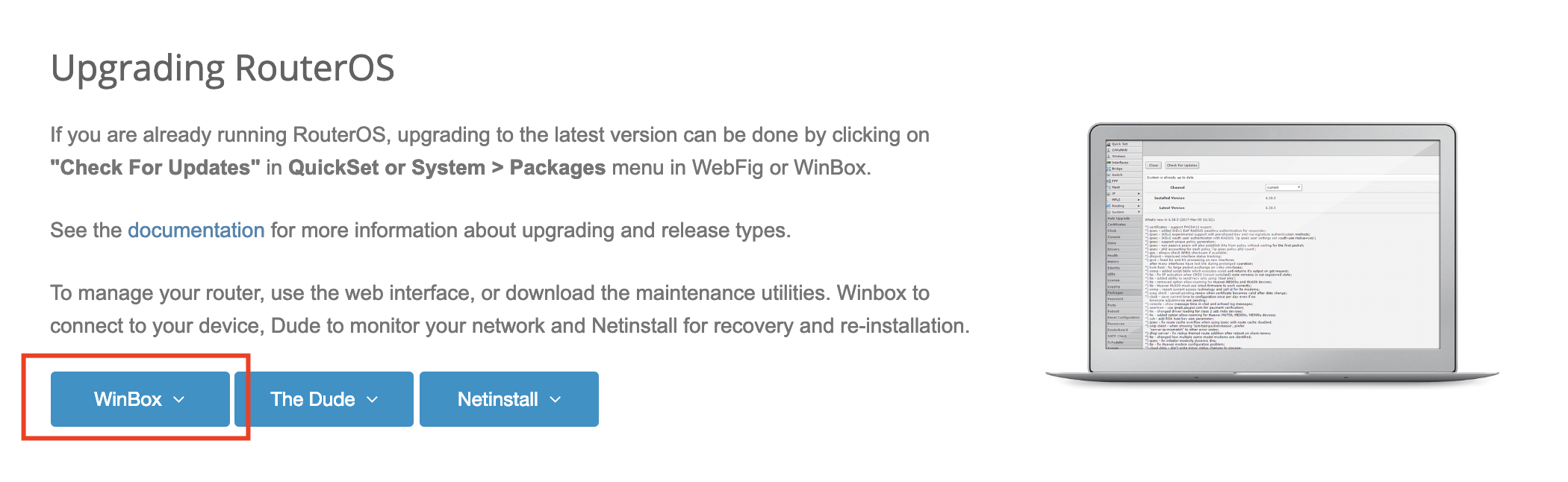
5. Then run the whole script. You should see this effect if the machine will be created with no issues:



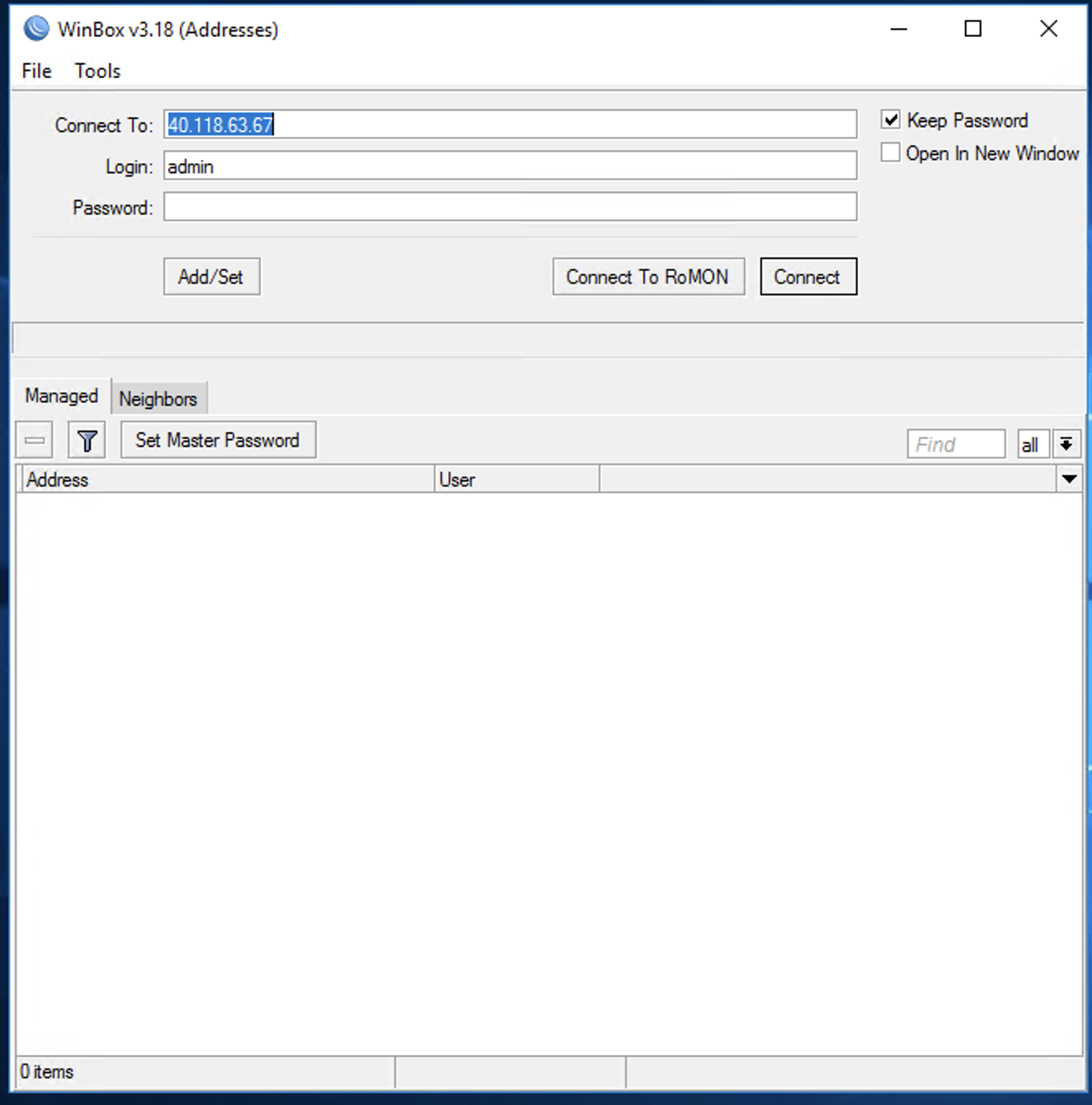
**Task 3: Configure MikrotikVM**

1. Sign in the Azure portal at https://portal.azure.com
2. Download WinBox on your Windows machine: <https://mikrotik.com/download>

(I am using the Virtual Machine for this purpose)

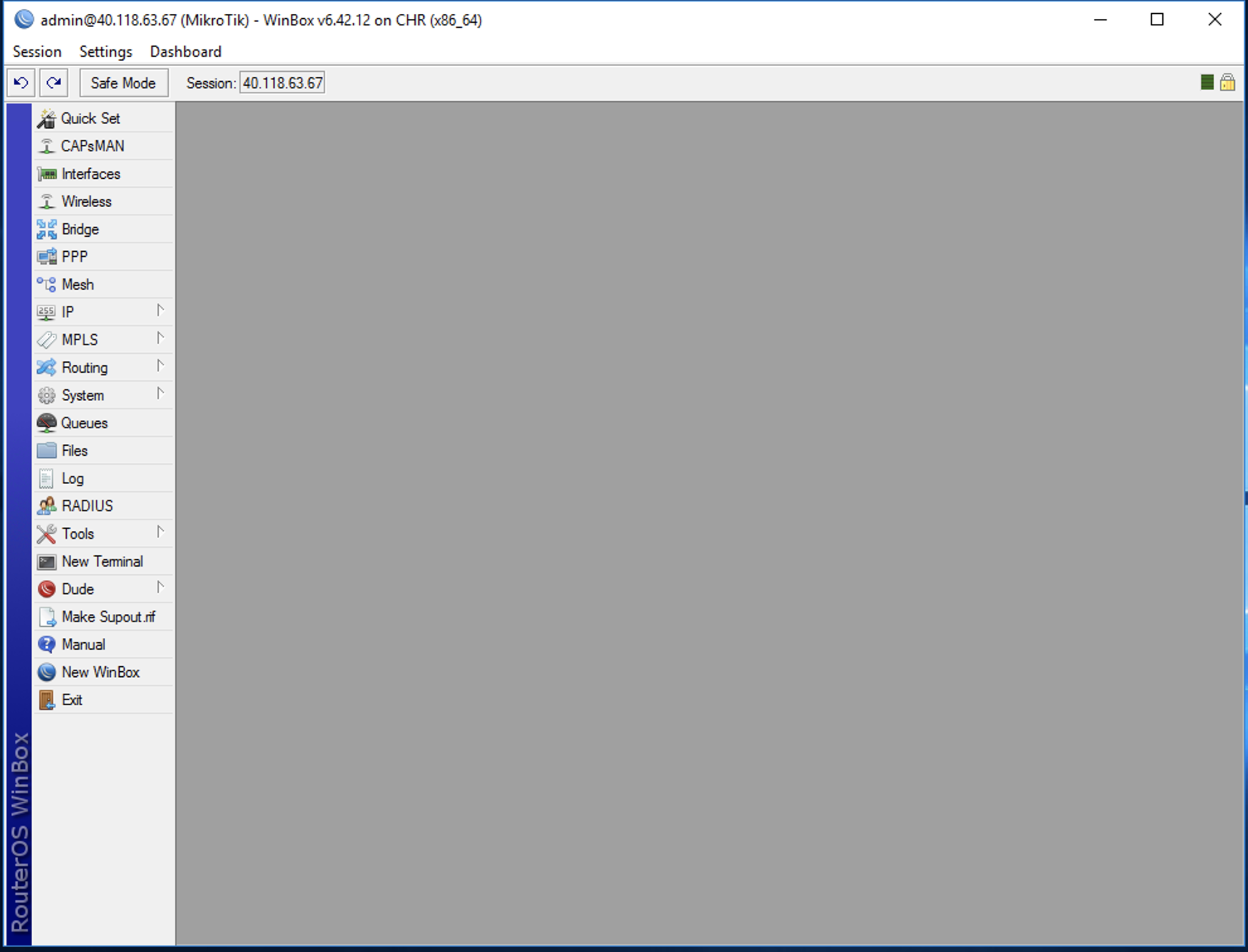
****

1. Run WinBox, put the IP address of Mikrotik and click Connect



Please remember, by default Mikrotik image comes with empty password for admin user name. I strongly recommend you change the default password by doing this procedure: https://wiki.mikrotik.com/wiki/Manual:Securing\_Your\_Router

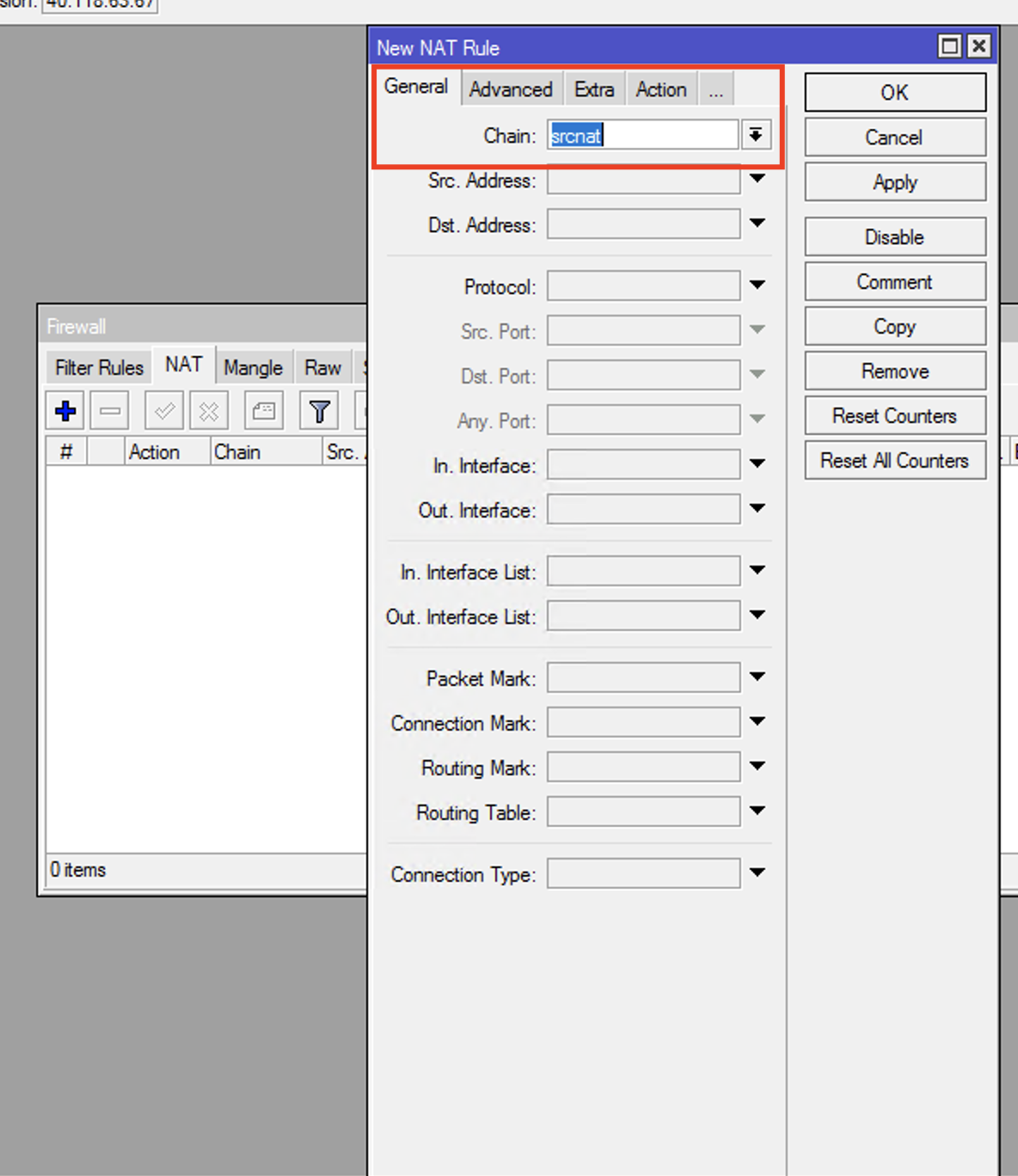
1. After successful connection you should see image like this:



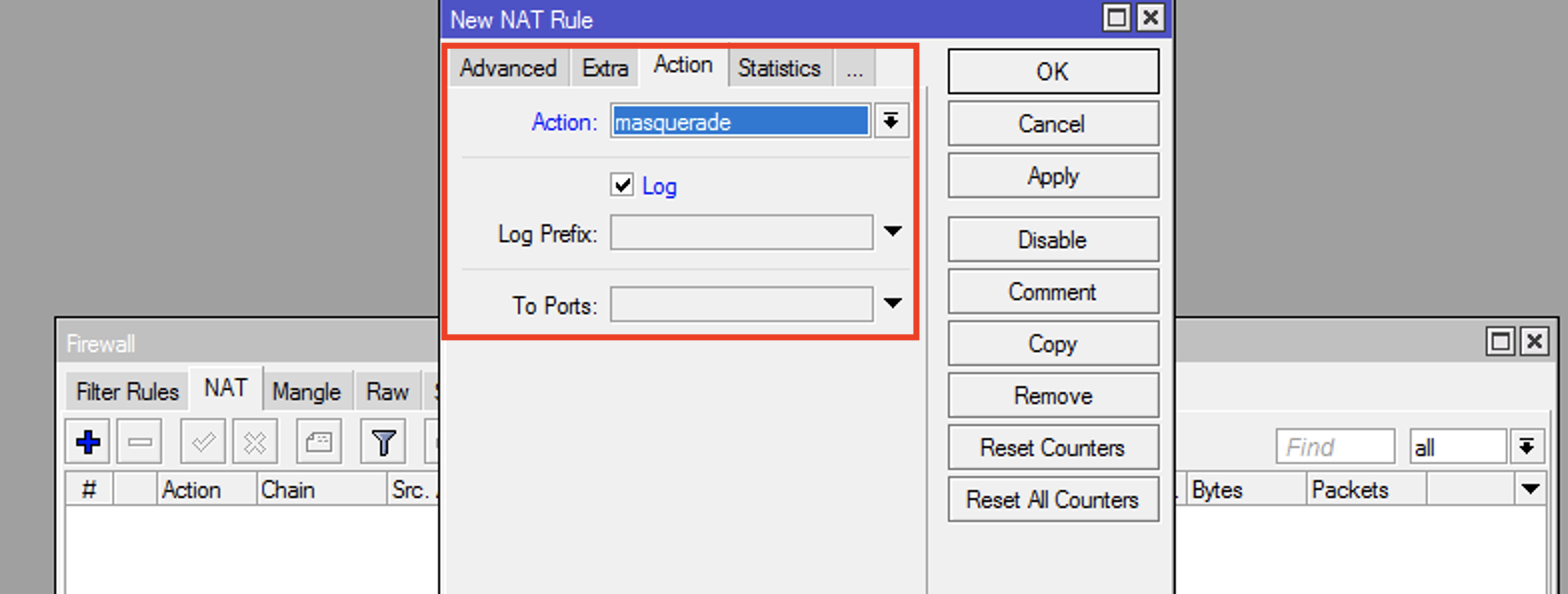
This proves that you have managed to connect to Mikrotik and can manage the router settings.

1. On the left menu go to **IP -> Firewall** and then to **NAT** section
2. Add new entry (by choosing plus icon on top of the bar) and configure options in the following way:

* **General -> Chain** -> srcnat

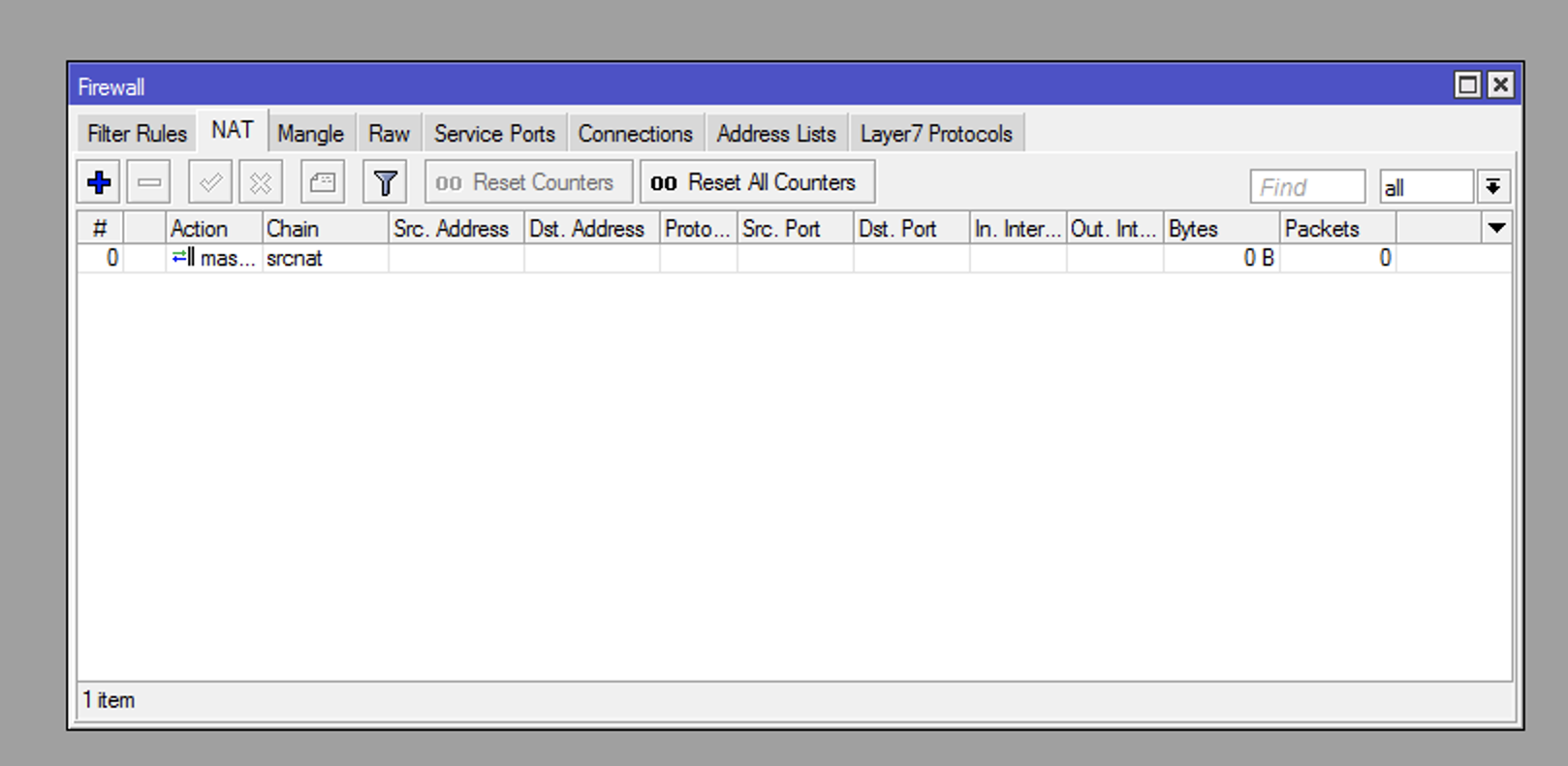


* **Action -> Action** -> masquerade
* **Action -> Action** -> Log (mark)



1. This is all you need to setup on **Mikrotik**.

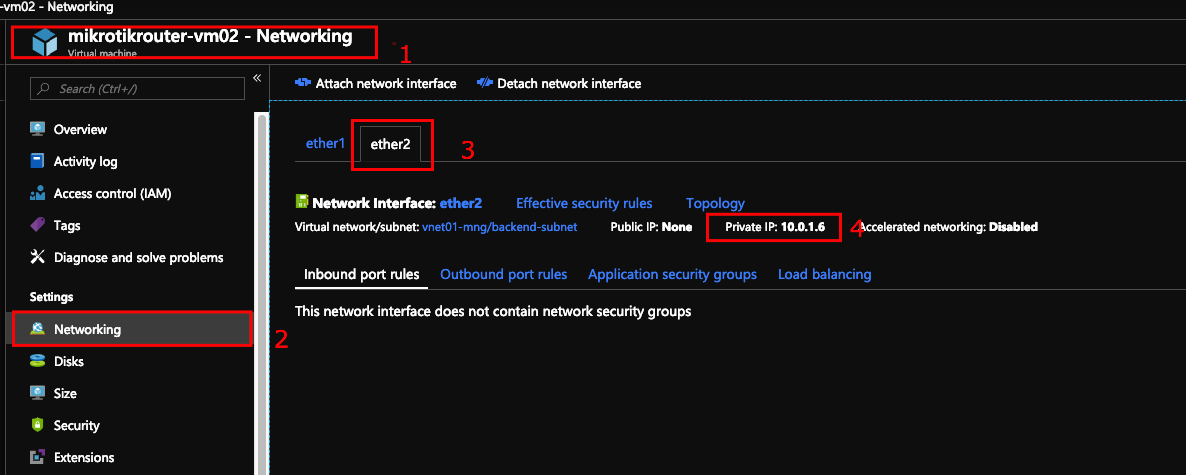
The final config should look like this:



1. To validate that the routing works fine, go to Connections and wait before we will setup the routing table in another Task. In the Connections tab you will be able to diagnose all connections which will go through this router.

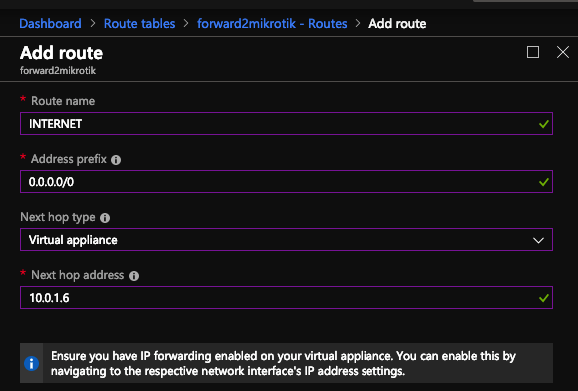
**Task 4: Configure UDR on subnet with Ubuntu VM**

1. Before you will start, double check the private IP address attached to the second interfaces (the one without Public IP) on Mikrotik.



1. Please open Virtual Machines blade and choose the VM ubuntu01, which we have mentioned at the very beginning of this lab.
2. Check the subnet in which this VM works and write it down.
3. Create new Route table by going to Create a resource and choose Route table
4. When the new route table is ready, open it and add two options:
   1. **Routes**

* Route Name: INTERNET
* Address Prefix: 0.0.0.0/0
* Next hop type: Virtual appliance
* Next hop address: <PRIVATE ADDRESS of second card of Mikrotik router – the one without public ip address assigned>



* 1. **Subnets**
* Click Associate button
* Choose the VNET and SUBNET to which you want to assign routing table.

Please assign this to subnet in which your ubuntu01 vm is working.

1. After this step the routing table has been added and we can test it.

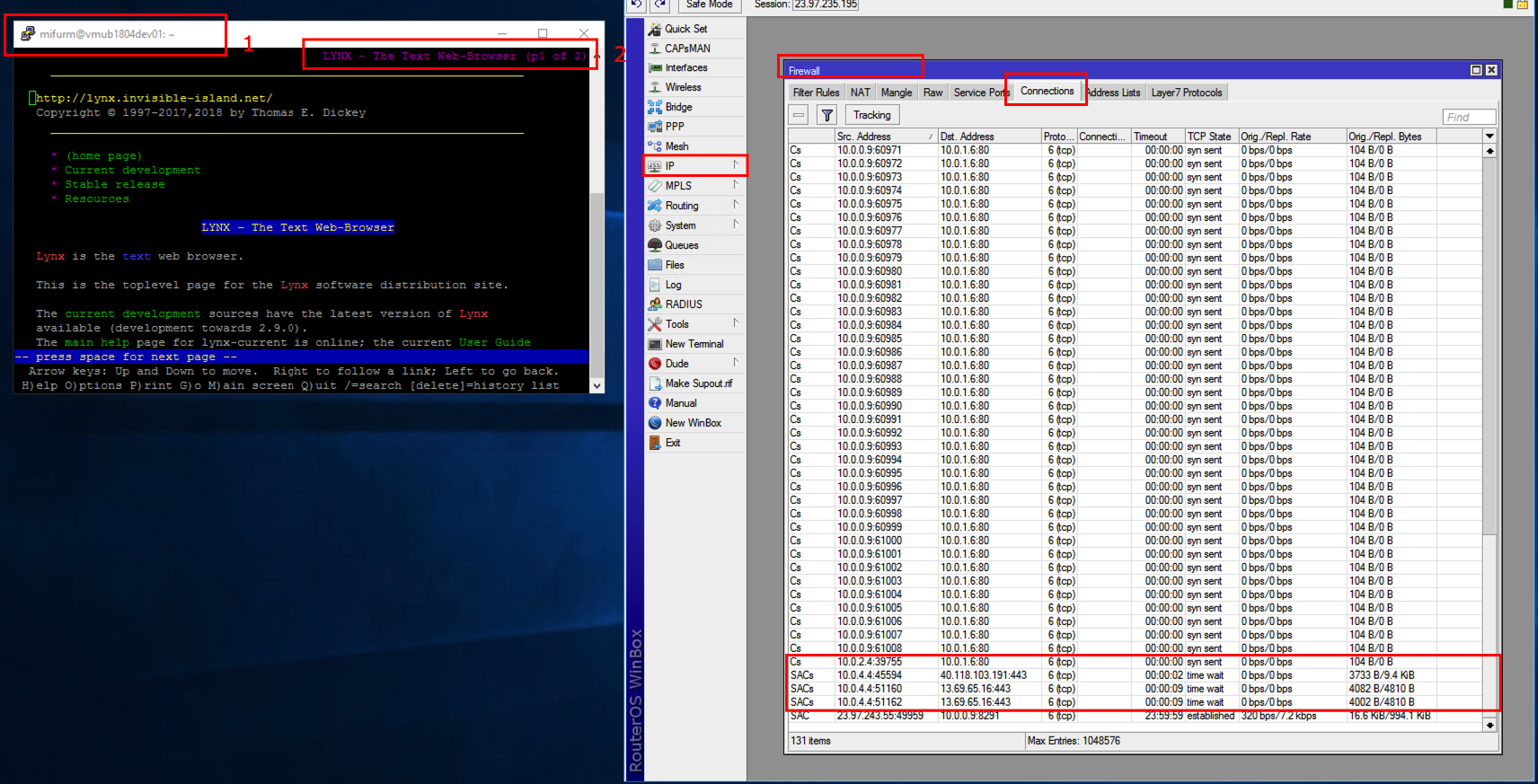
Be carefull – as you have redirected the whole traffic to Internet, you will not be able to log into your ubuntu machine from the public IP address. The best option will be to use another VM in the same VNET, from which you can access ubuntu01 vm using it’s private address.

I am using the same Windows virtual machine, from which I was connected to router.

1. On the ubuntu01 VM I am adding Lynx text browser to test the traffic.

You can addedd by using command: **sudo apt-get install lynx**

1. After installing Lynx, you can open Lynx by typing **lynx**
2. While the Lynx is connecting to the default site, in the WinBox tool in Connections, you should see outgoint connections from your ubuntu01 VM to Internet going through the routerVM.



1. You can use other options on Mikrotik to filter traffic or route the traffic. NVA (Network Virtual Appliacances) are way more convenient in traffic routing the Route Tables in Azure. Azure Route Tables can only be assigned on the subnet level and route the whole traffic on subnet. In NVA’s you can be more precise and route the traffic from single VM, group of VM’s to other device. You can also filter the traffic.

**LAB Summary**

In this lab you have learned how IP Forwarding works and how you can use it with NVA (based on Mikrotik)