PRISMA
BY PALO ALTO NETWORKS

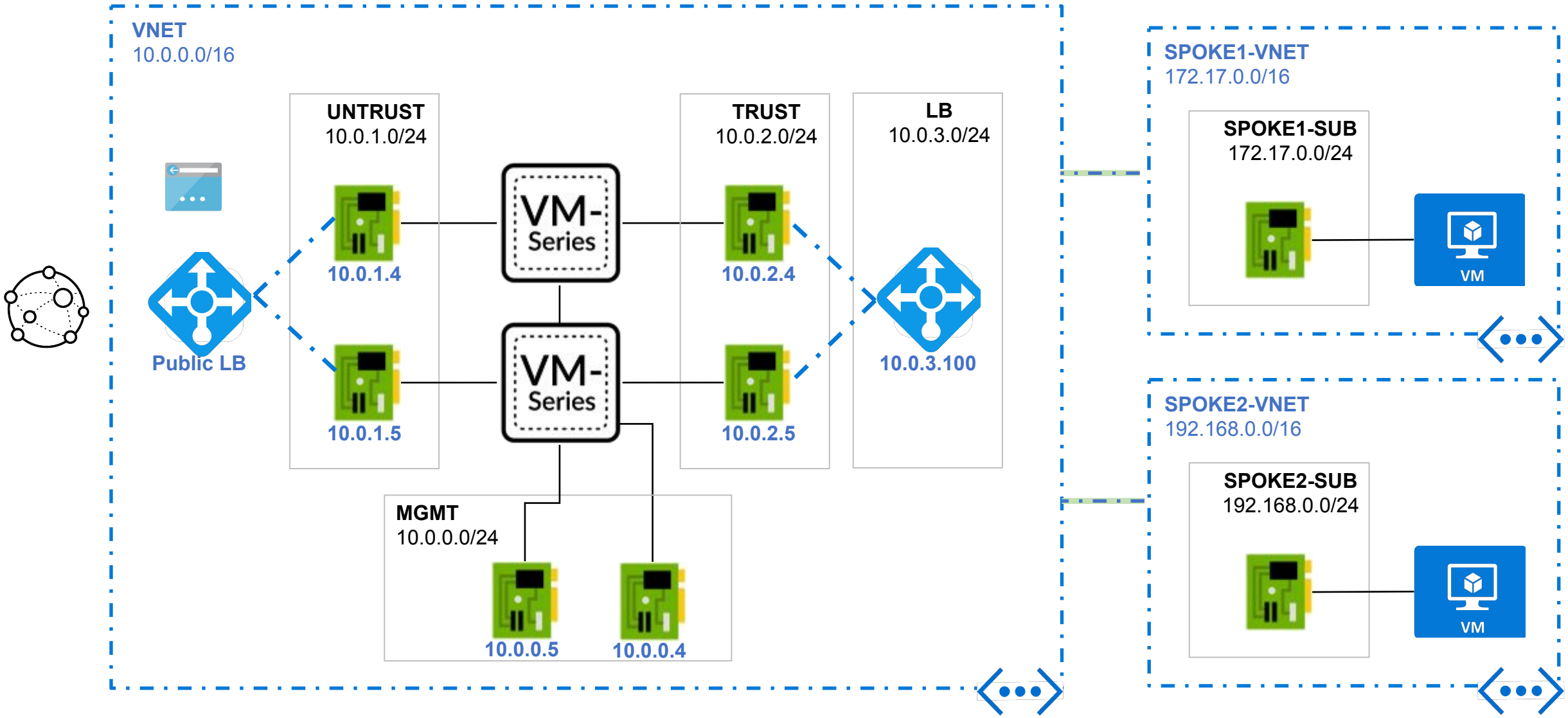
Prisma Public Cloud - Azure

Lab Guide

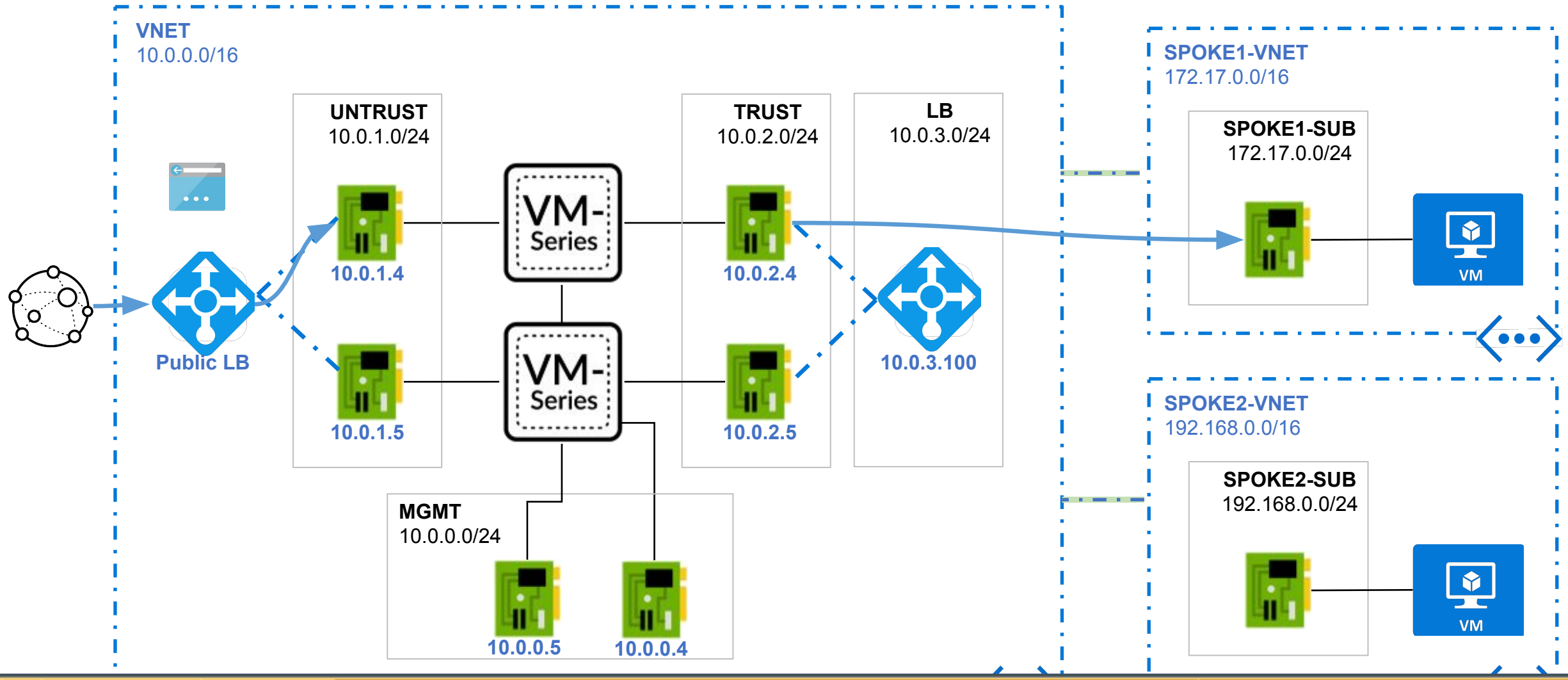
paloalto NETWORKS

Lab Design

Overall Design

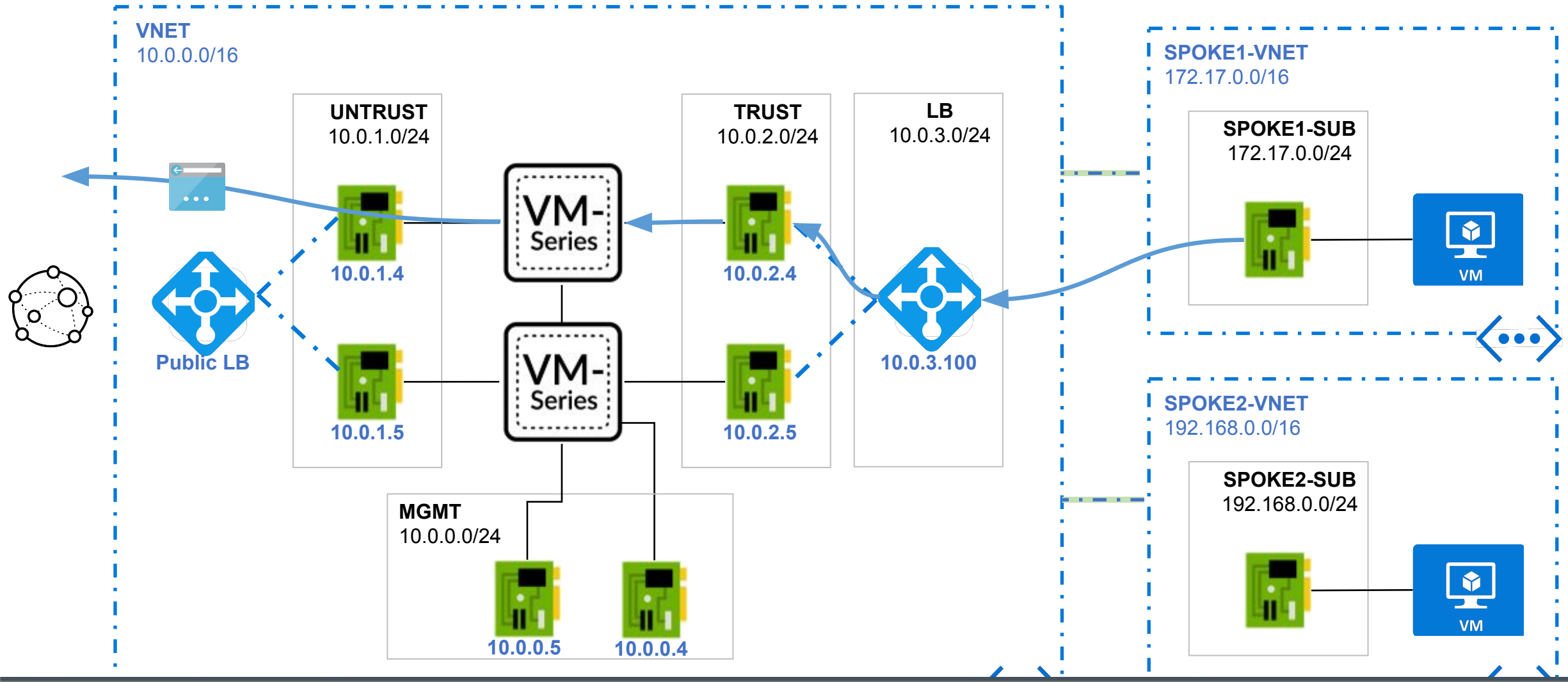


INBOUND TRAFFIC FLOW



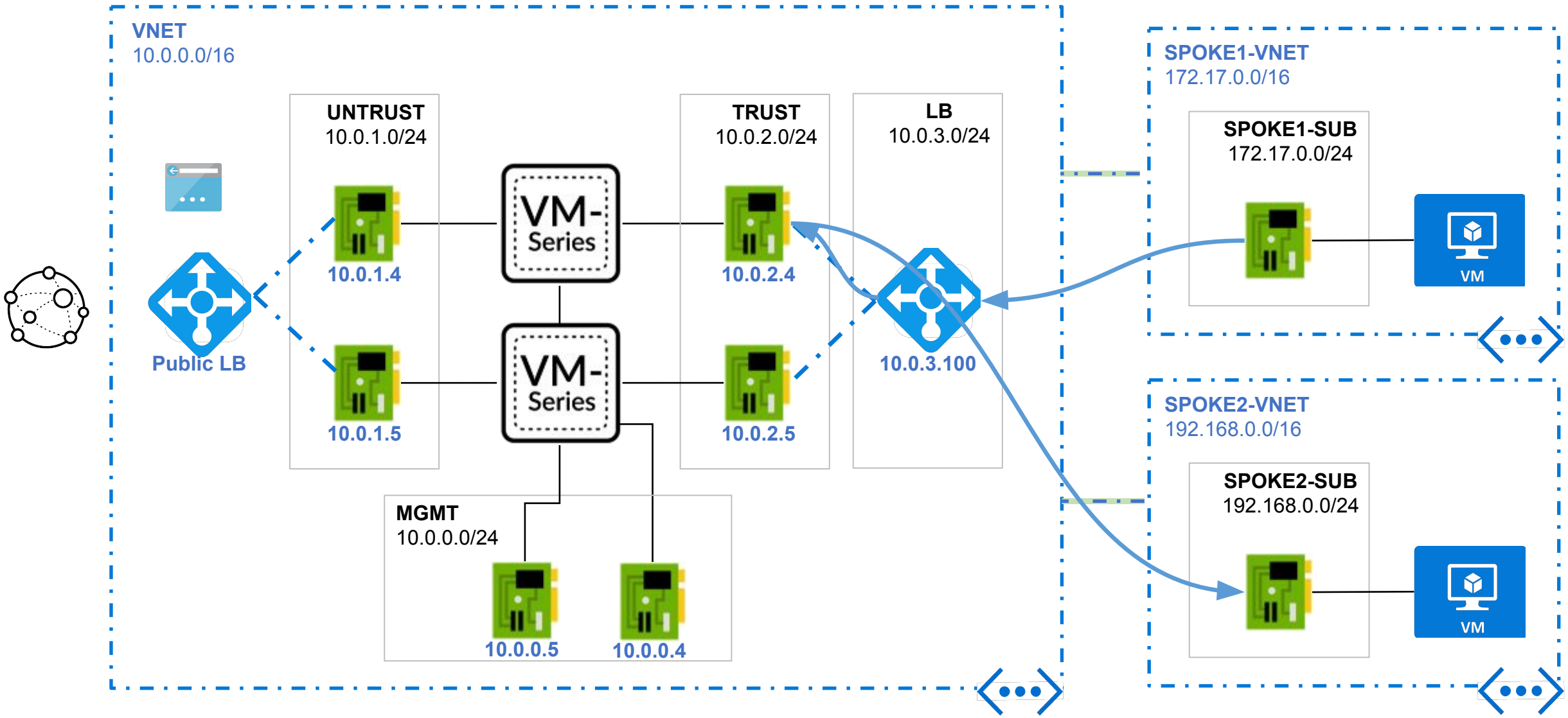
			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
2	inbound-spoke1	none	untrust-zon...	untrust-zone	any	any	untrust-nic	any	dynamic-ip-and-port ethernet1/2	destination-translation address: spoke1-vm

OUTBOUND TRAFFIC FLOW



			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
3	outbound	none	trust-zone	untrust-zone	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

EAST-WEST TRAFFIC FLOW

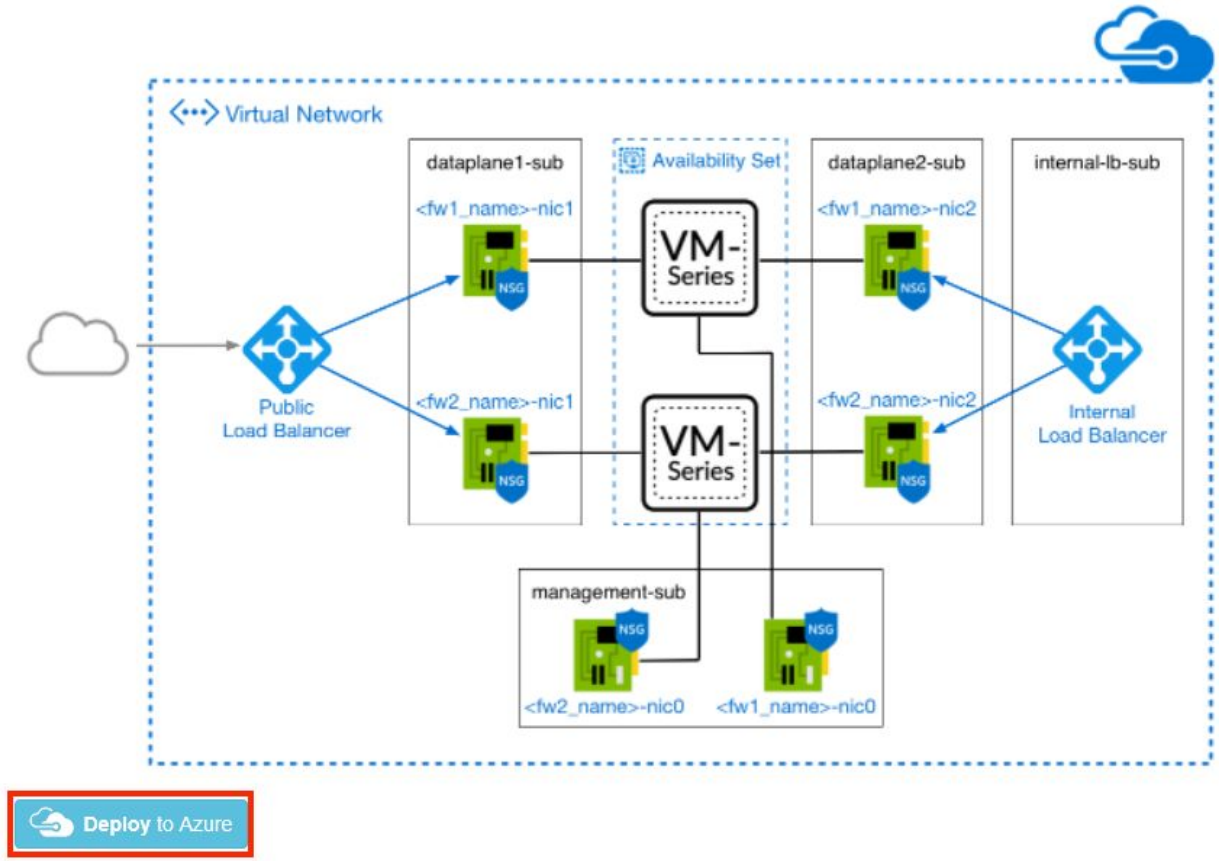


Deploy environment

Deploy Environment

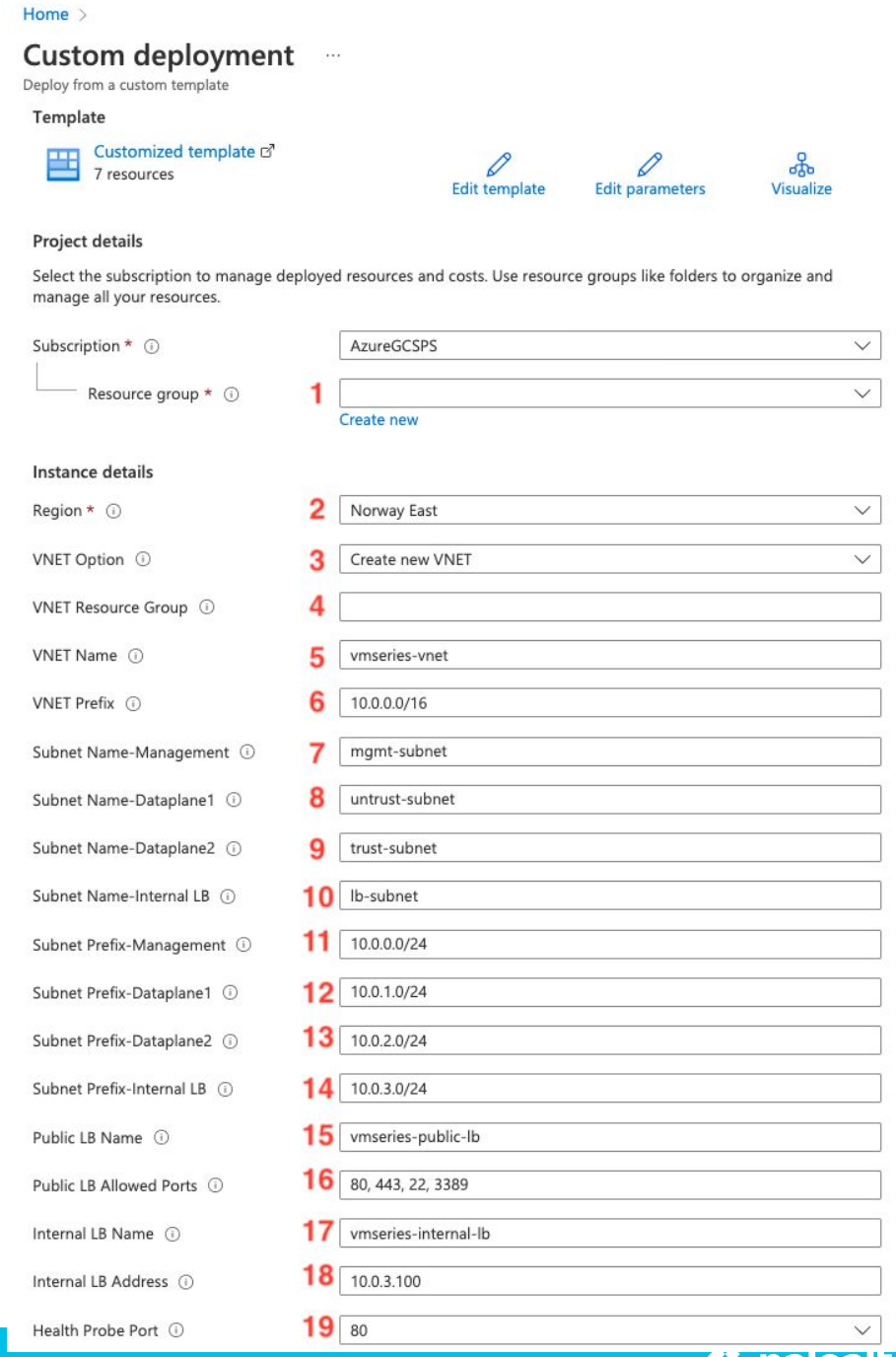
1. Click on the Link
   https://github.com/PaloAltoNetworks/lab-azure-vmseries

2. Click on “Deploy to Azure”



Deploy Environment 1/2

1. Create a new Resource Group: Azure-Lab-<NAME>
2. Select any Region
3. Select “Create new VNET”
4. Empty
5. VNET-<NAME>
6. VNET Prefix (leave default)
7. Don’t Change
8. Don’t Change
9. Don’t Change
10. Don’t Change
11. Don’t Change
12. Don’t Change
13. Don’t Change
14. Don’t Change
15. Don’t Change
16. Don’t Change
17. Don’t Change
18. Don’t Change
19. Don’t Change



Deploy Environment 2/2

1. No need to change
2. Don’t Change
3. Don’t Change
4. Don’t Change
5. No need to change
6. Don’t Change
7. Don’t Change
8. Don’t Change
9. Change to **“Bundle 1”**
10. Leave Default
11. Don’t Change
12. Don’t Change
13. Don’t Change
14. Don’t Change
15. Change to **“enable”**
16. Don’t Change
17. Don’t Change
18. Don’t Change
19. Don’t Change
20. Change to your preferred Username
21. Type a strong Password

Admin/Admin2 is not a Valid Username

Deploy Environment

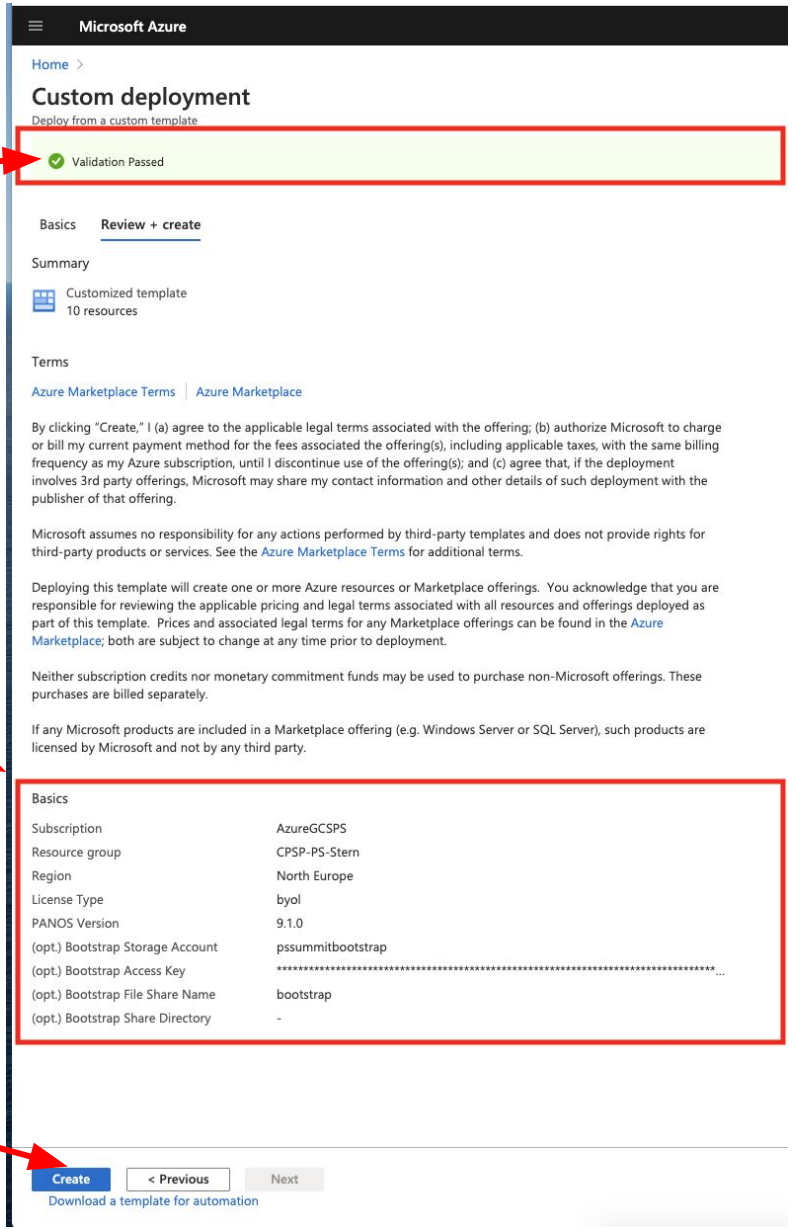
Check the box and click **“Next: Review + create”**

Deploy Environment

Check that the “Validation Passed”

Validate/Review the configuration

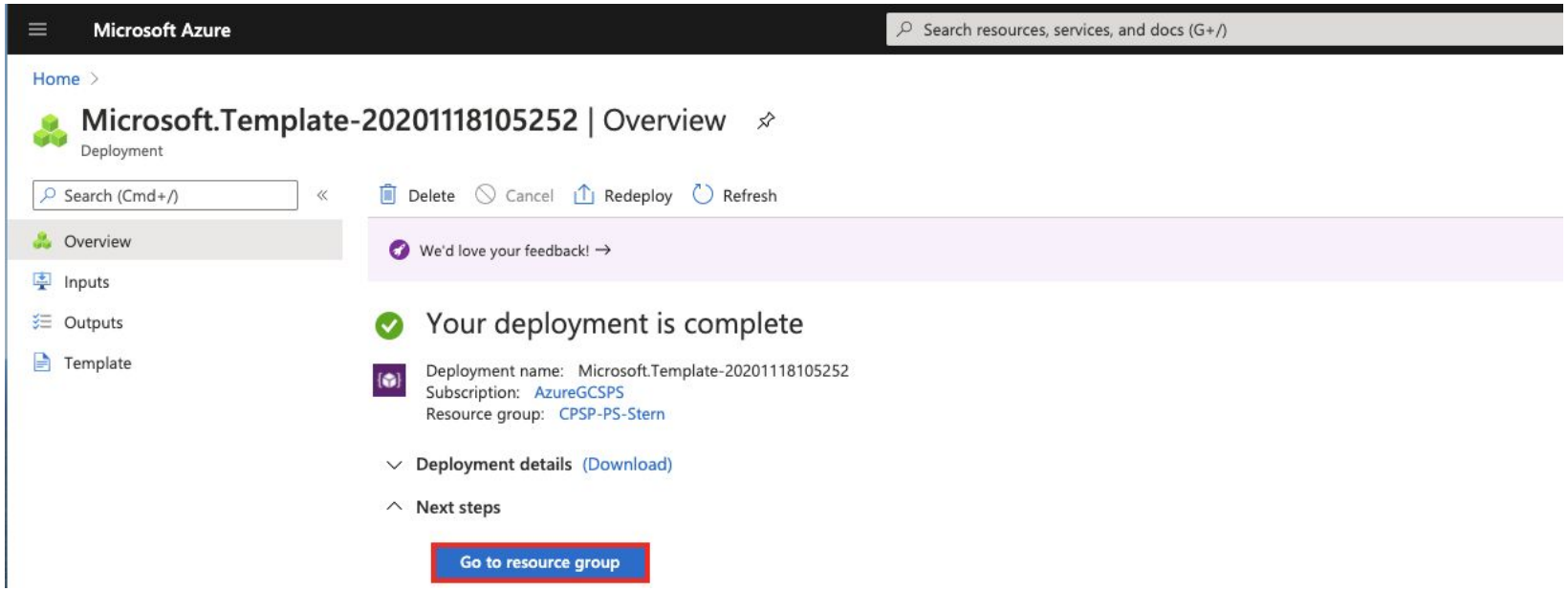
Click **“Create”**



Deploy Environment

- Click on “Go to resource group” when your deployment is complete.
  - See below

Deployment can take up to 30 min! Coffee break!



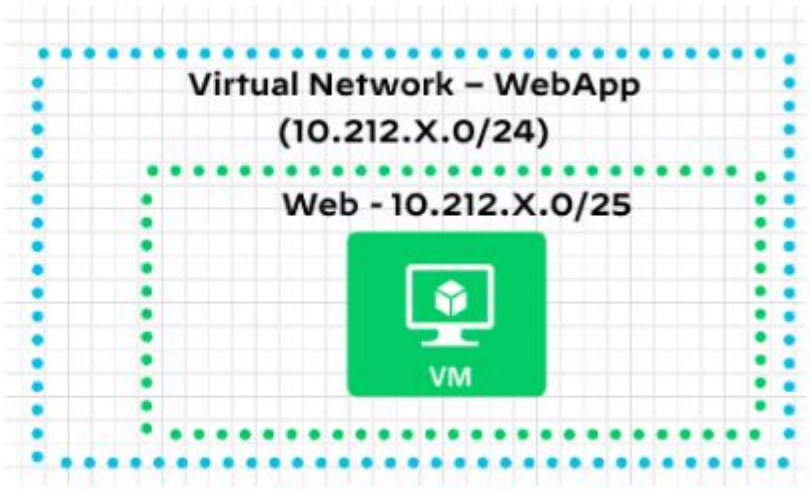
Deploy WebApp Resource Group

Deploy WebApp

1. Click on the Link to get to the GitHub Repository

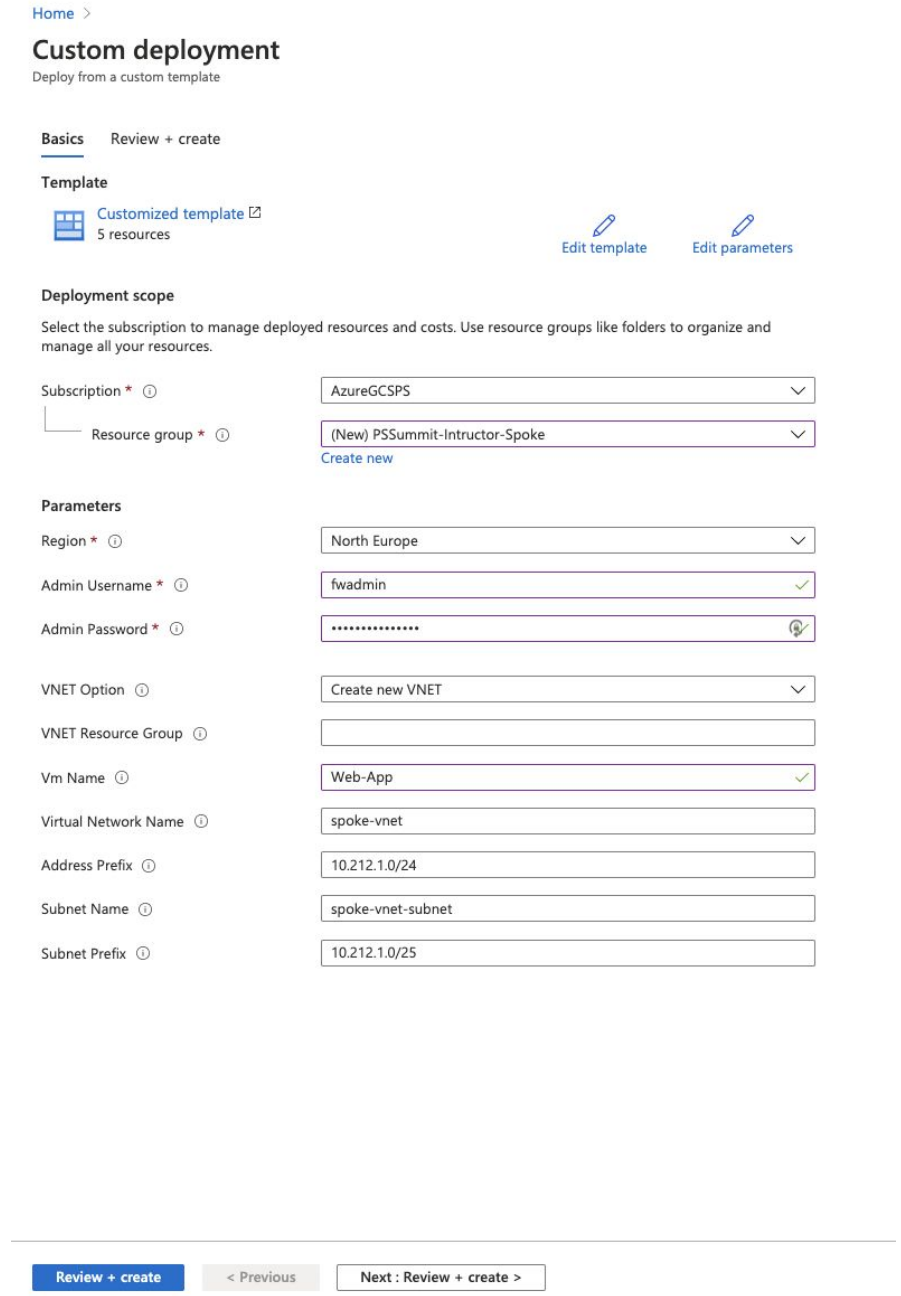
   https://github.com/PaloAltoNetworks/lab-azure-vmseries

2. Click on “Deploy to Azure”



Deploy WebApp Spoke

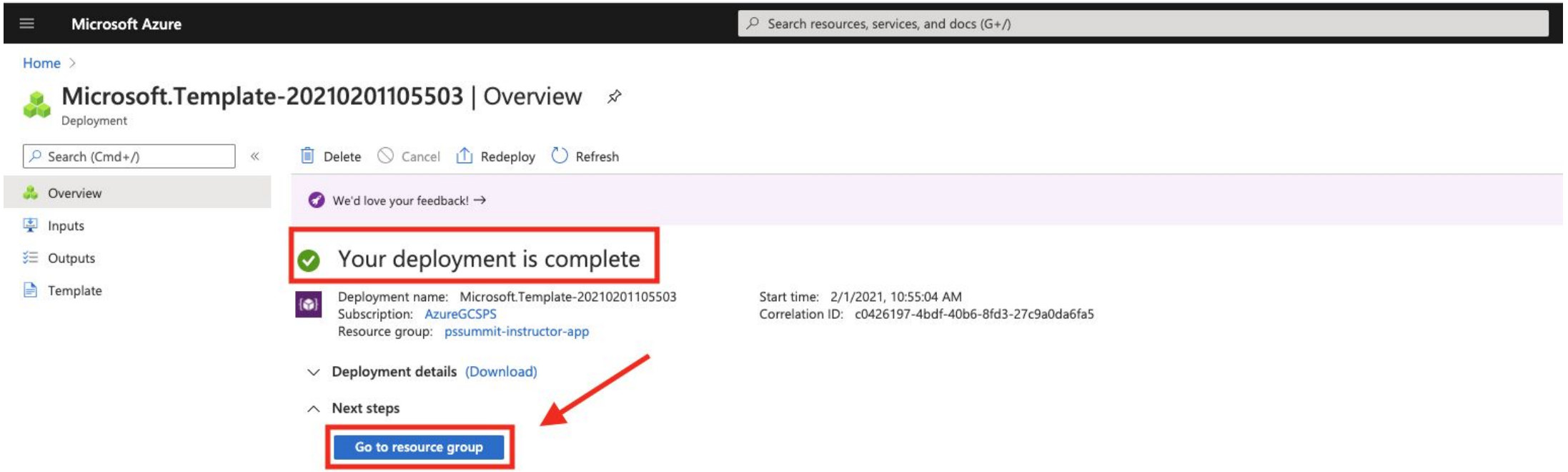
1. Create a new Resource Group (Azure-Lab-Spoke1<NAME>
2. Select any Region
3. Your prefered Username
4. Your prefered Password
5. Select “Create new VNET”
6. Empty
7. Web-App-<Name>
8. VNET-Spoke-<Name>
9. Don’t Change
10. Don’t Change
11. VNET-Spoke-subnet<Name>
12. Don’t Change



Deploy WebApp Spoke

- Click on “Go to resource group” when your deployment is complete.
  - See below

Deployment can take up to 10 min including VM boot!



Next Steps

1. **Create Virtual Network Peerings** between the newly deployed “Hub” and any applications Virtual Networks.
2. **Create a Route Table** in the Application Virtual Networks to forward traffic to the “Egress Private IP” which is the Private IP of the Internal Load Balancer.
    - For instance “0.0.0.0/0” to “Egress Private IP” for Outbound / East-West Traffic
3. **Configure Web-App Server** to simulate a Web Server
    - Upgrade OS
    - Install Apache Web Server
    - Update Websites unique per Student

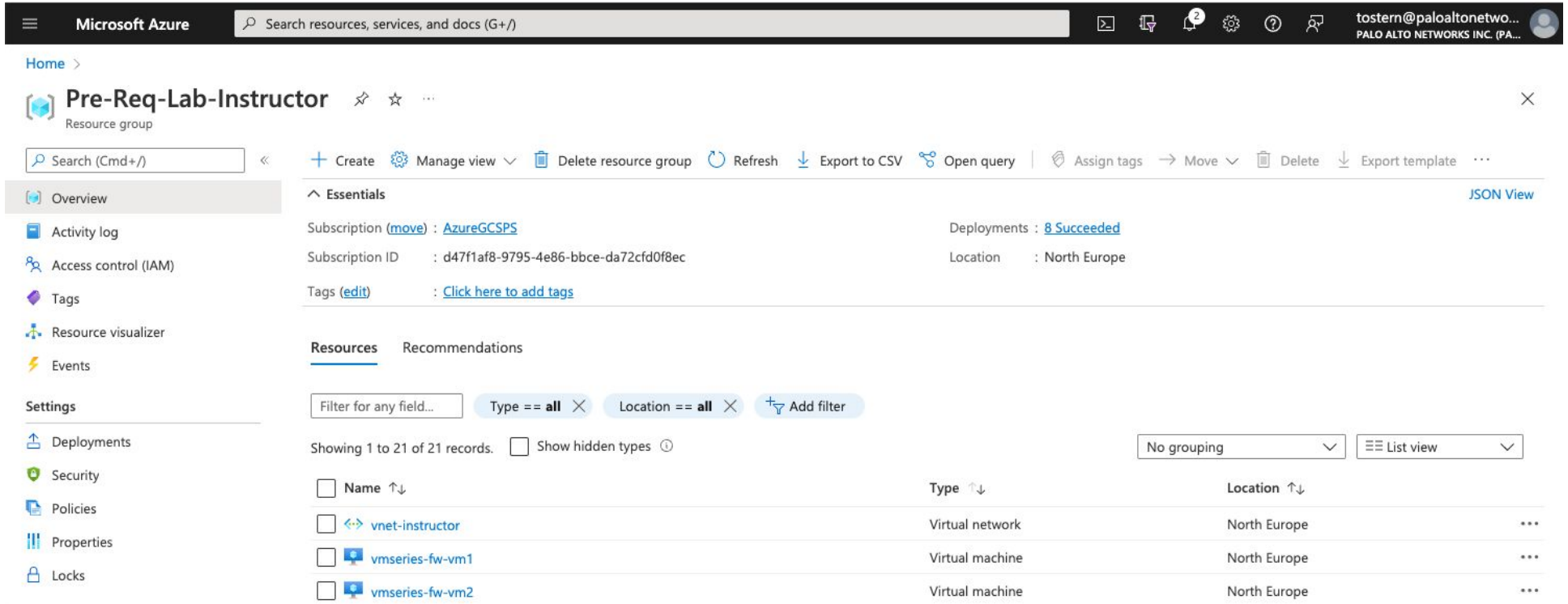
Configure VM-Series

Login into your Firewall

paloalto NETWORKS

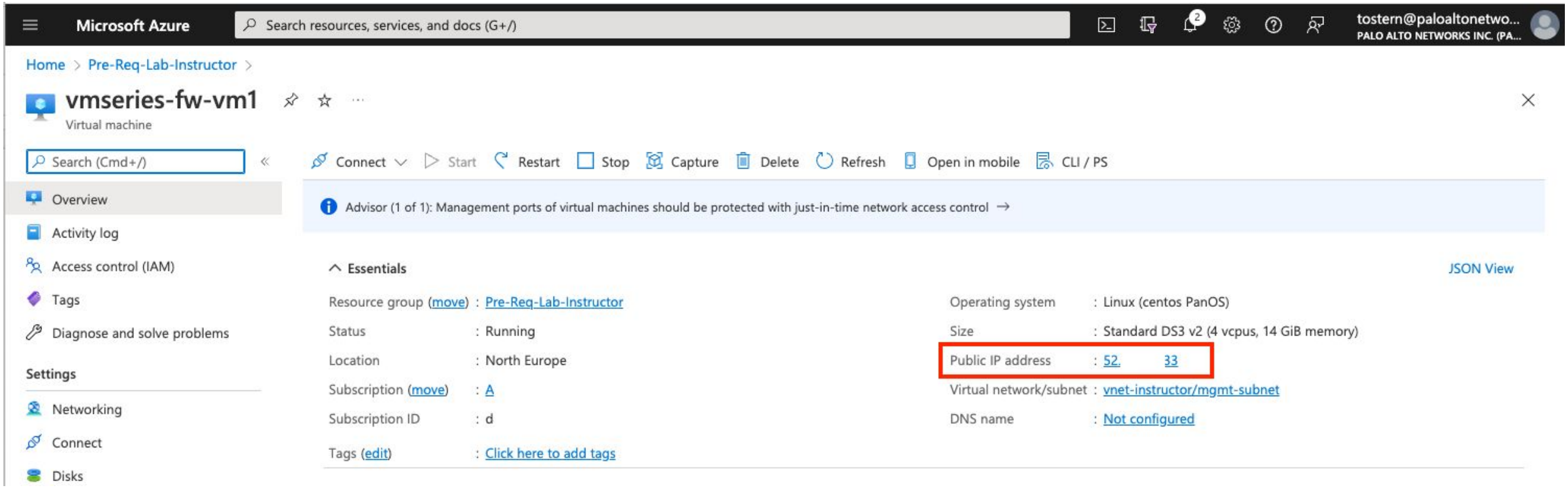
Login into VM-Series Firewall

- Go to your Resource Group you created in Slide 9
- Click on the first VM-Series firewall



Login into VM-Series Firewall

- In the Overview tab copy the “Public IP address”
- type in a new browser window the following **https://<Public IP>**

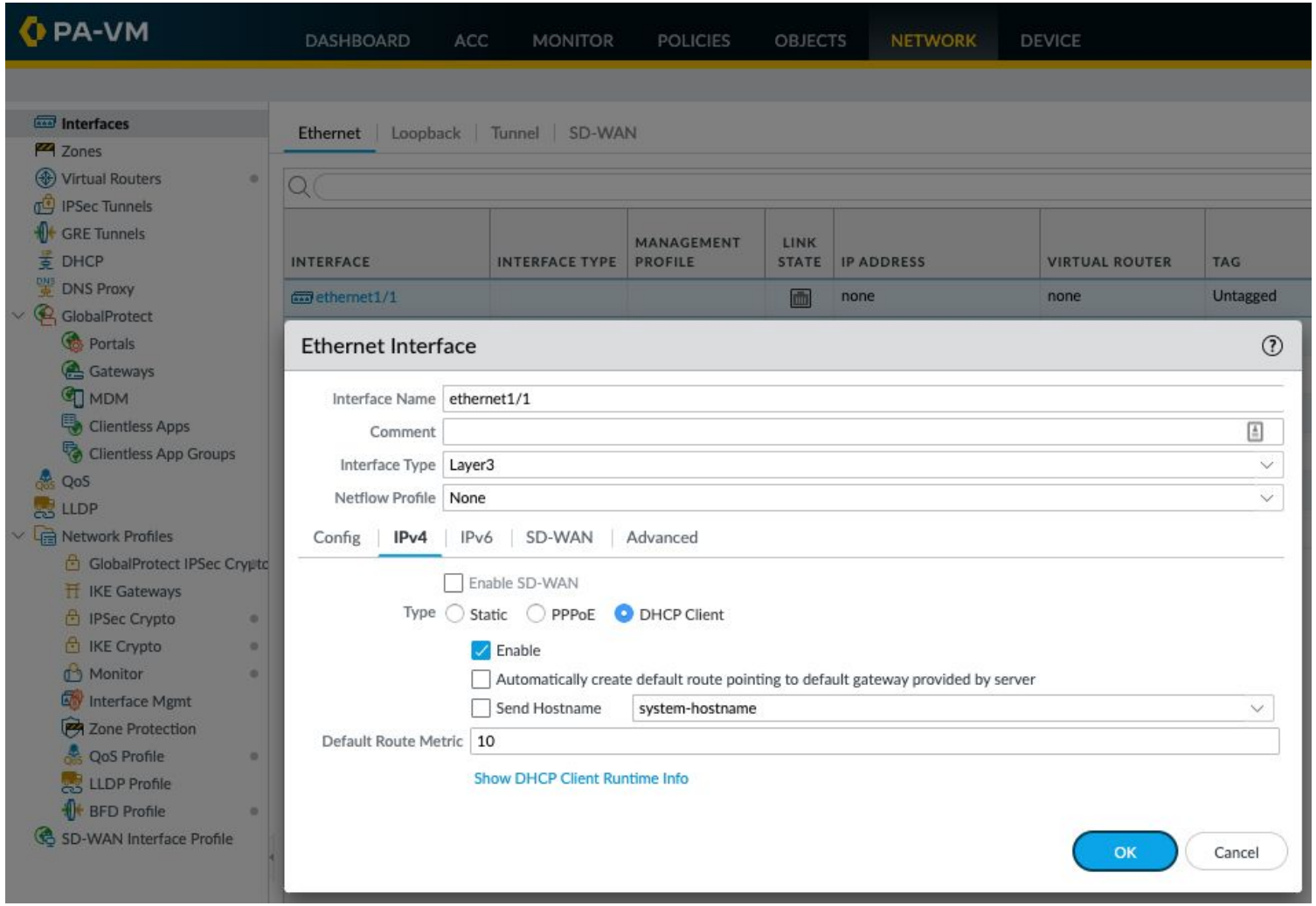


Configure VM-Series

Interface Configuration

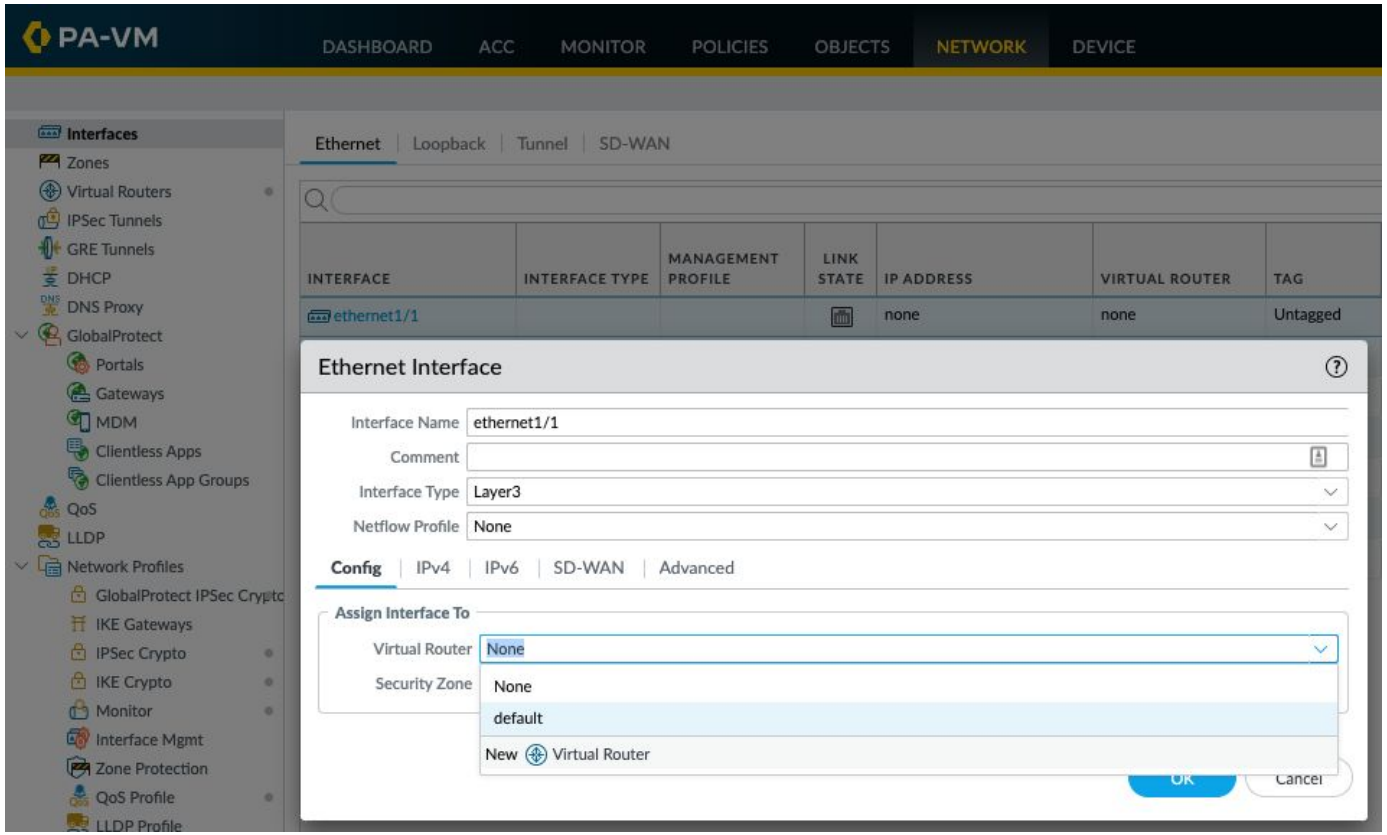
Configure Untrust Interface - IPv4

- Go to the Network tab
- Interfaces and select **“ethernet1/1”**
- configure the as shown on the picture



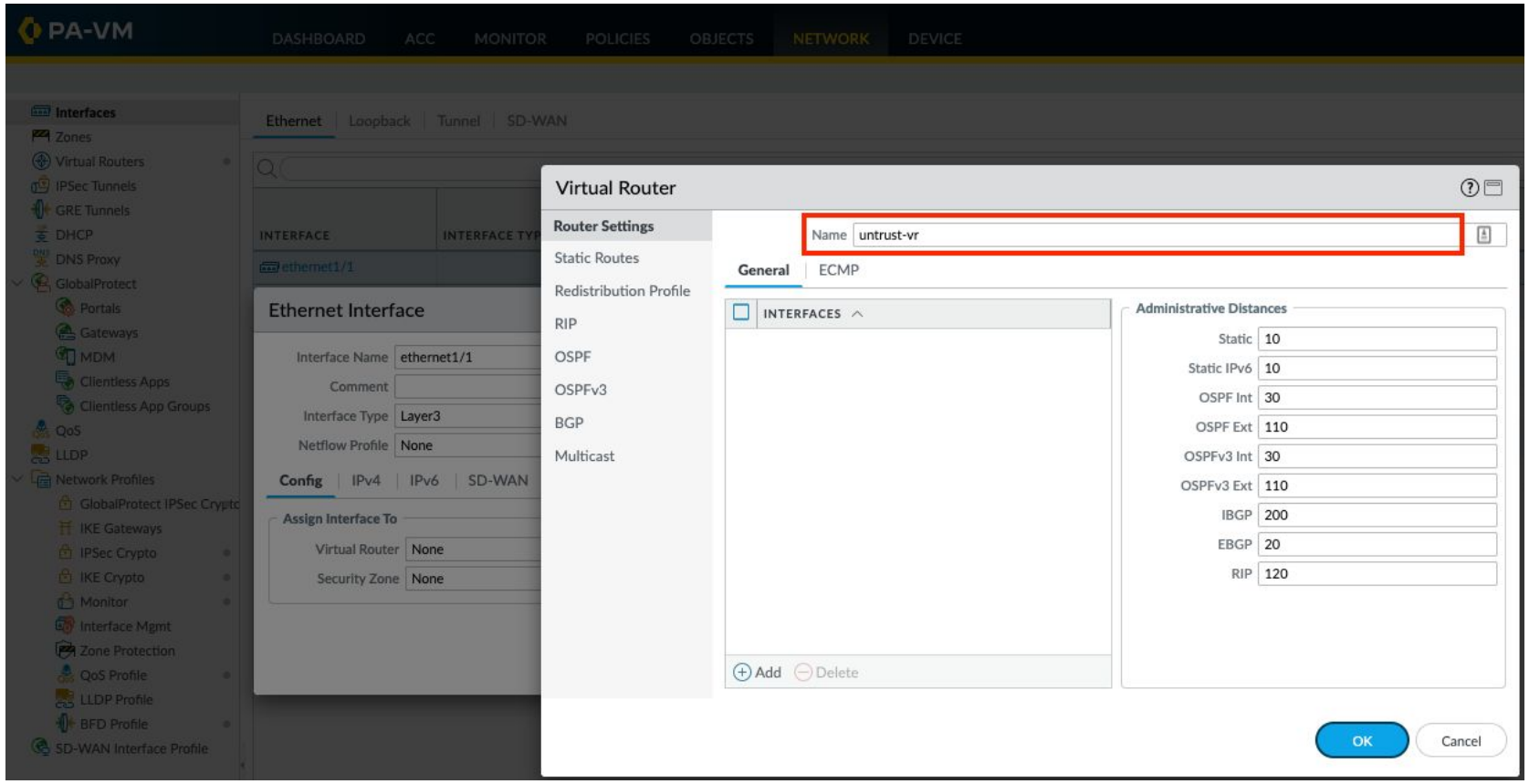
Configure Untrust Interface - Virtual Router

- In the Config tab of **“ethernet1/1”**
- configure the as shown on the picture
- Create a new virtual router



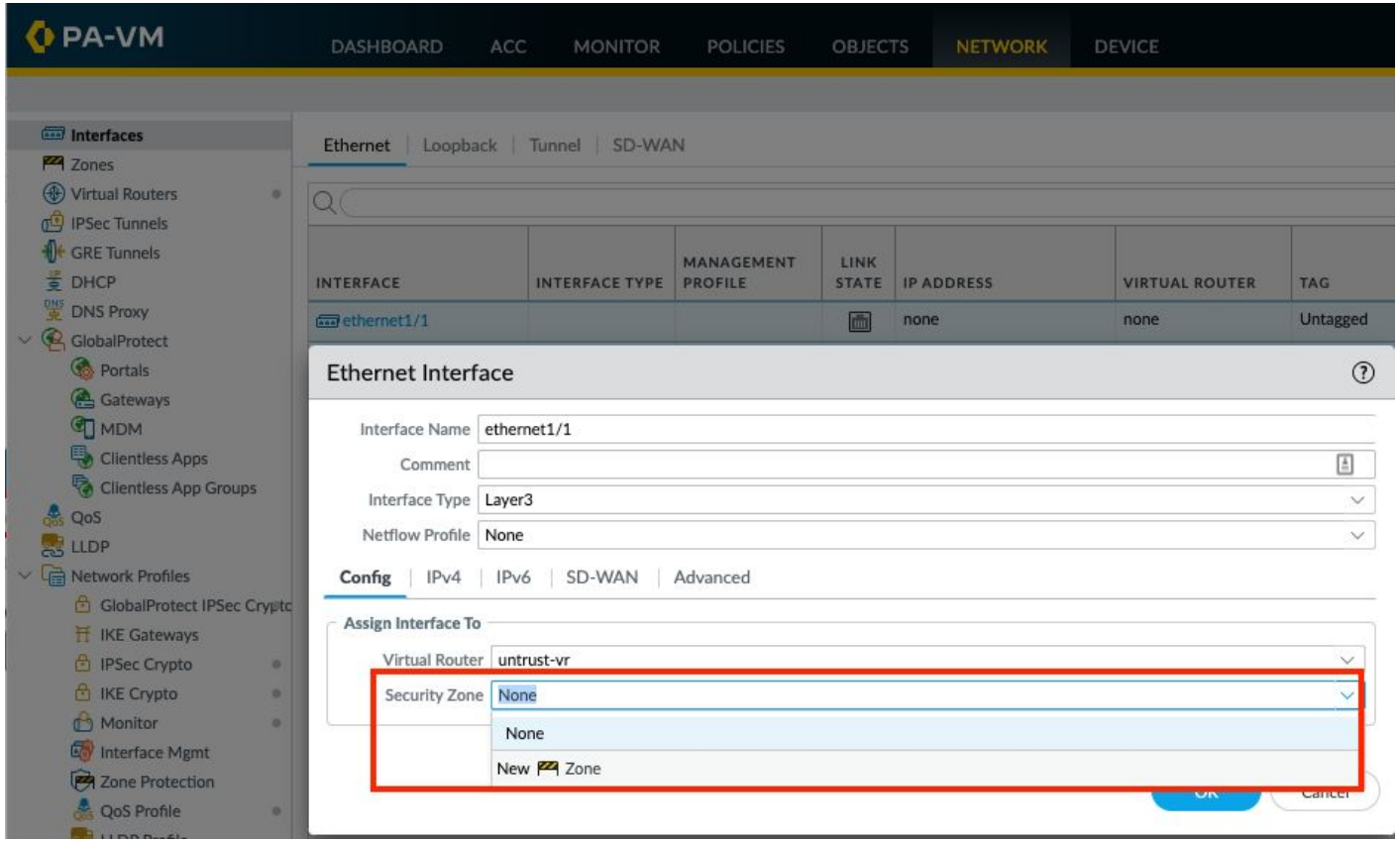
Configure Untrust Interface - Virtual Router

- provide a proper name
- select **“ok”**



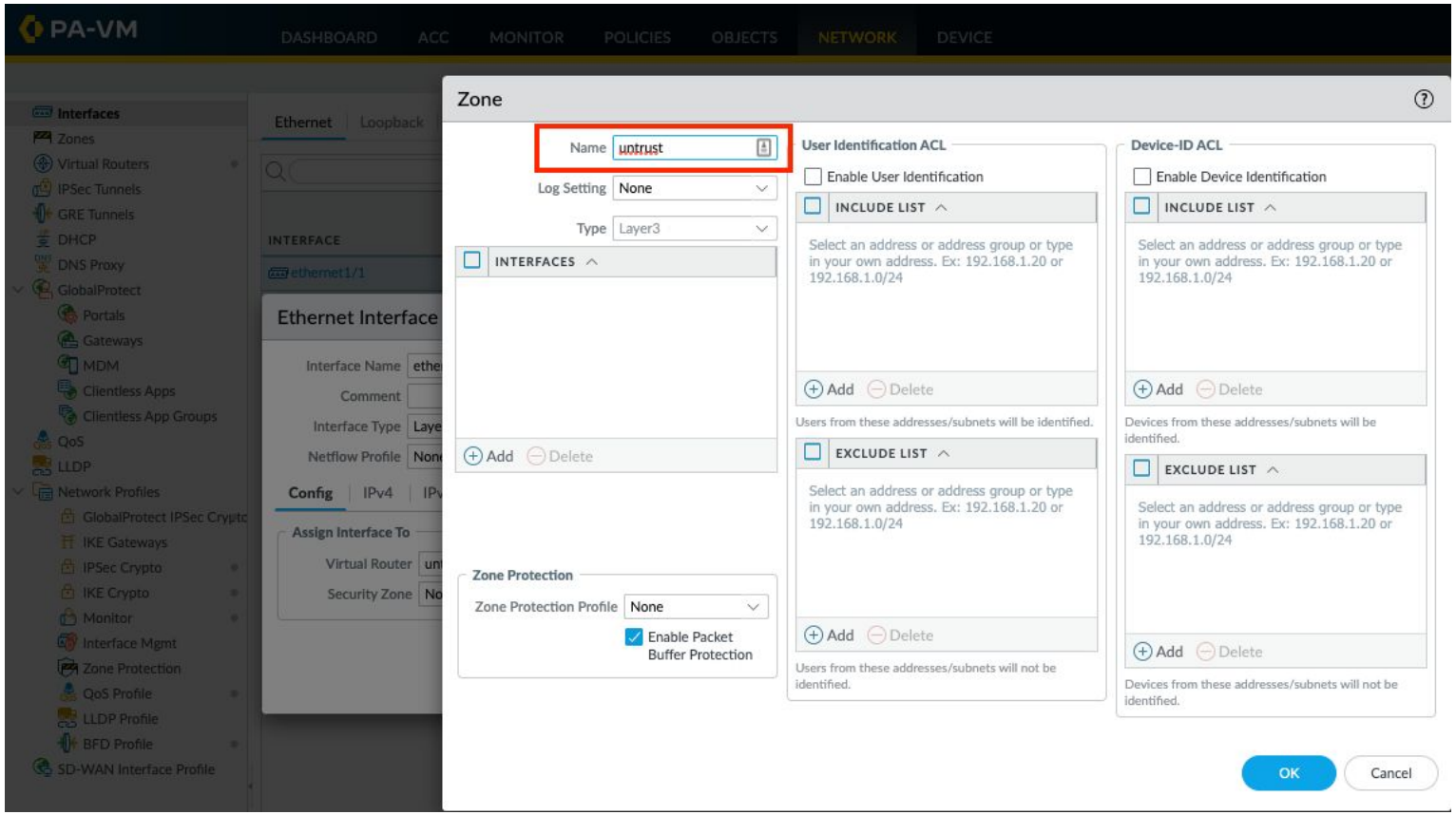
Configure Untrust Interface - Zone

- In the Config tab of **“ethernet1/1”**
- configure the as shown on the picture
- Create a new zone



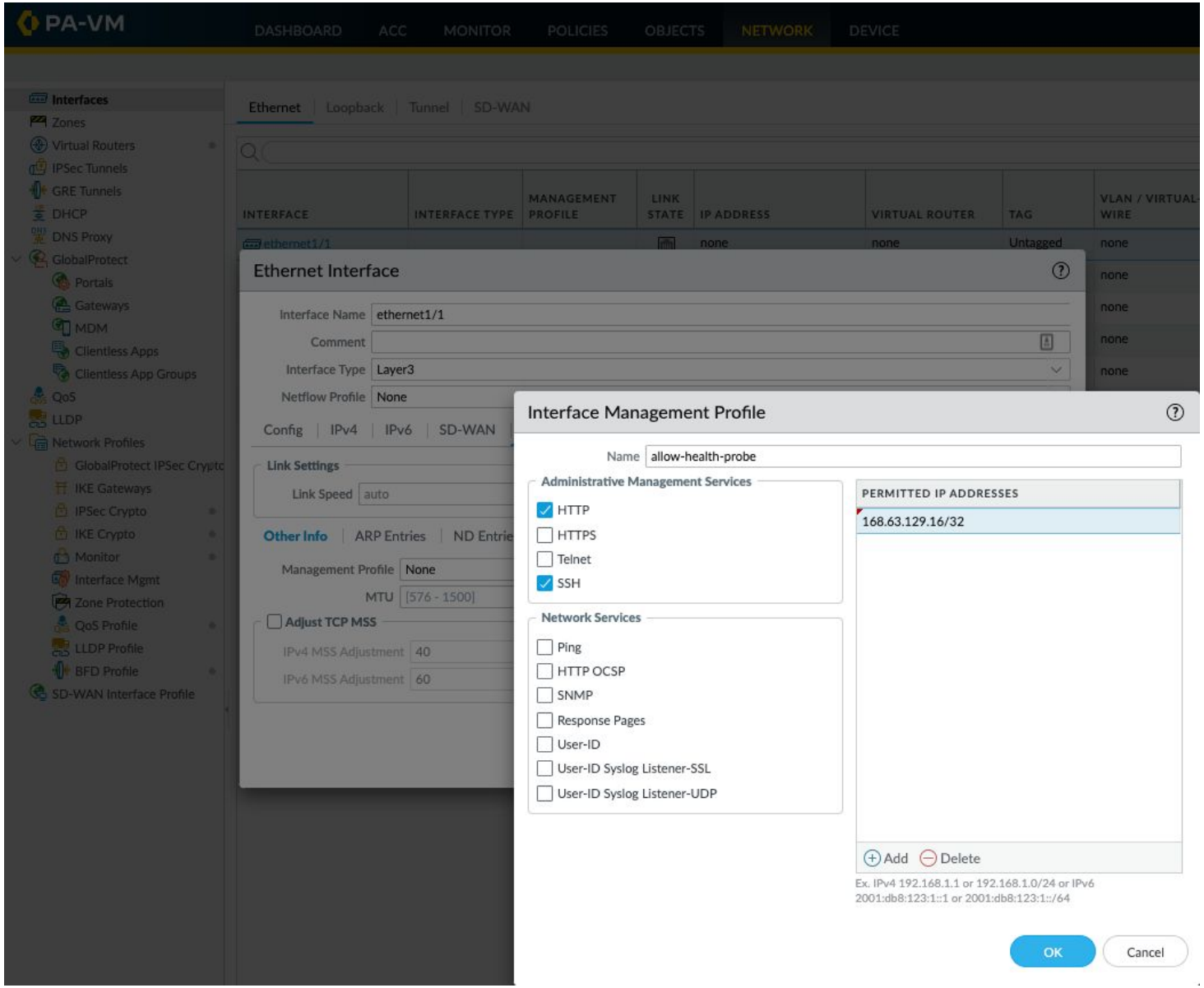
Configure Untrust Interface - Zone

- provide a proper name
- select **“ok”**



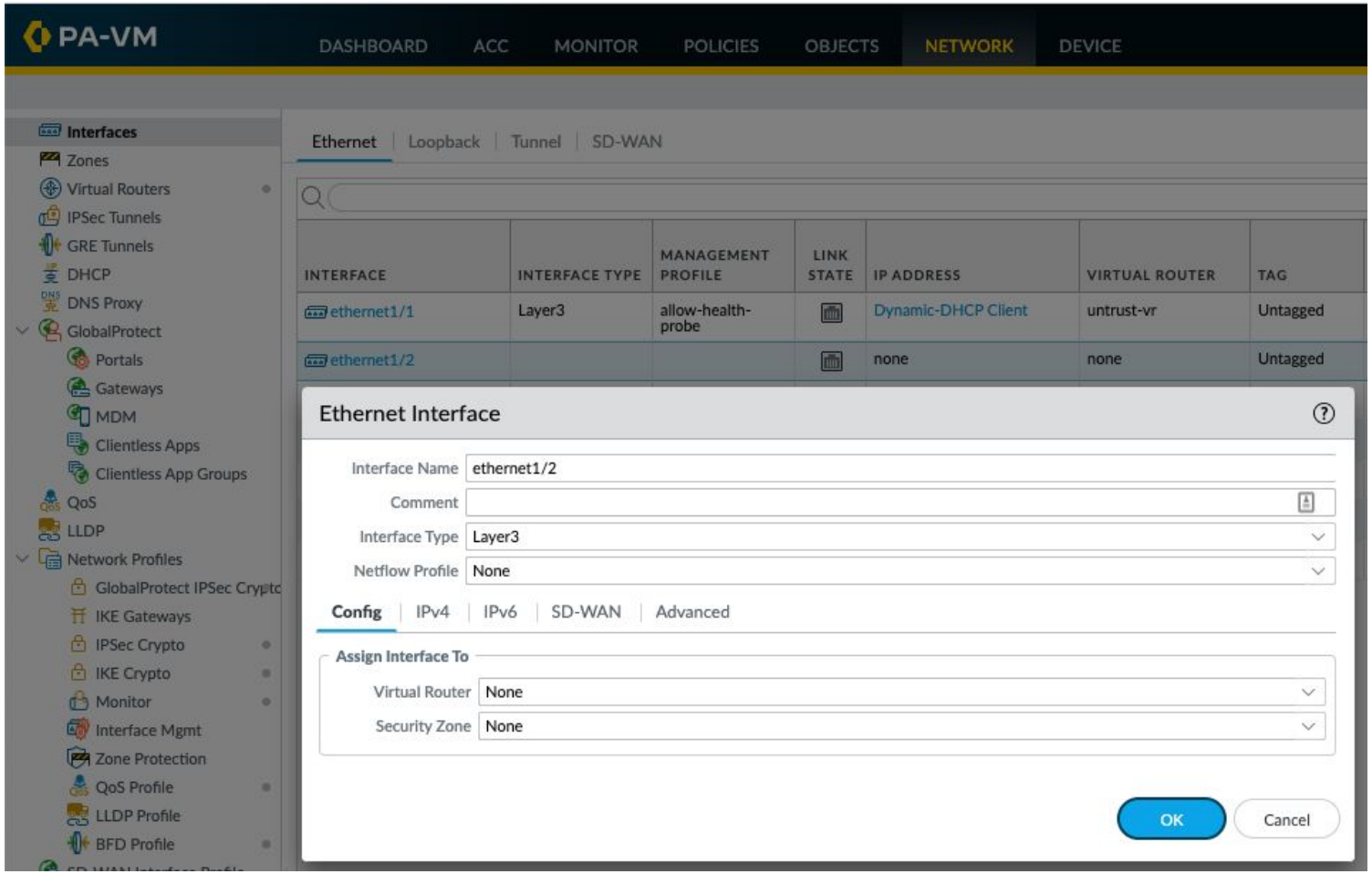
Configure Untrust Interface - Advanced

- While still inside eth1/1, click Advanced Tab
- Click the Management Profile dropdown and select “New Management Profile”
- Check SSH, HTTP
- Permitted IP: 168.63.129.16/32
- Click OK



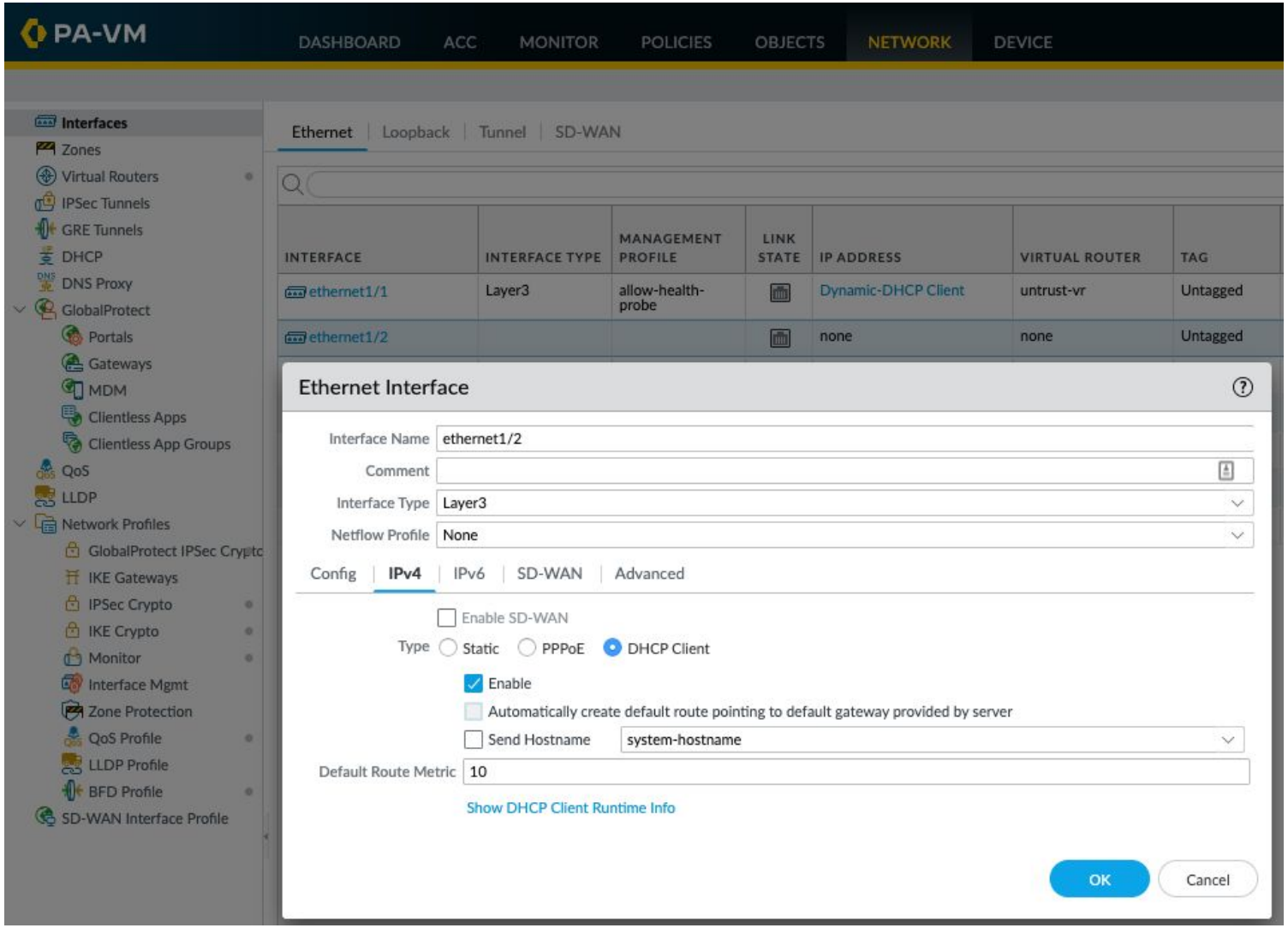
Configure Trust Interface - Config

- In the Config tab of **“ethernet1/1”**
- configure the as shown on the picture
- Create a new virtual router



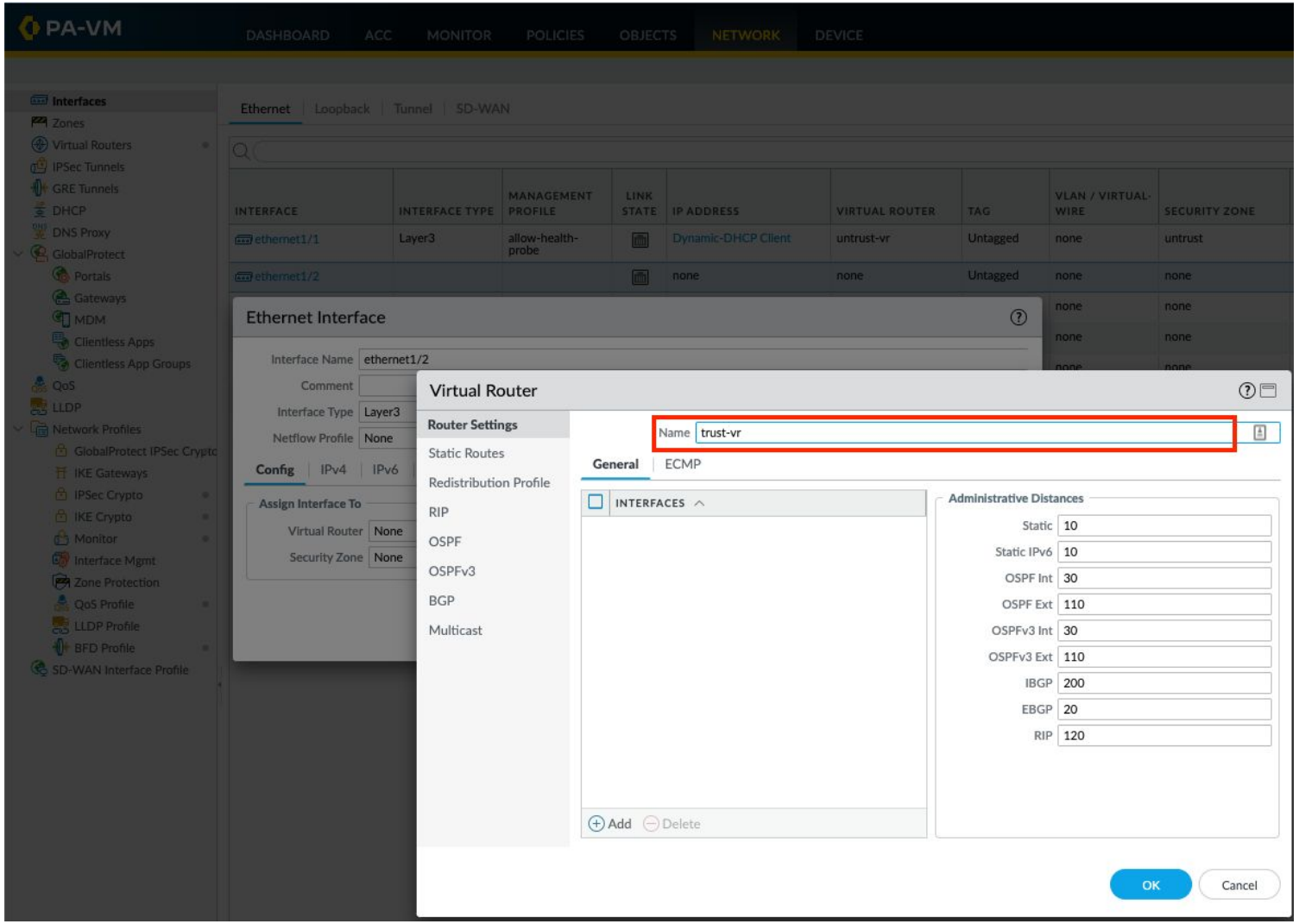
Configure Trust Interface - IPv4

- Go to the Network tab
- Interfaces and select **“ethernet1/2”**
- configure the as shown on the picture



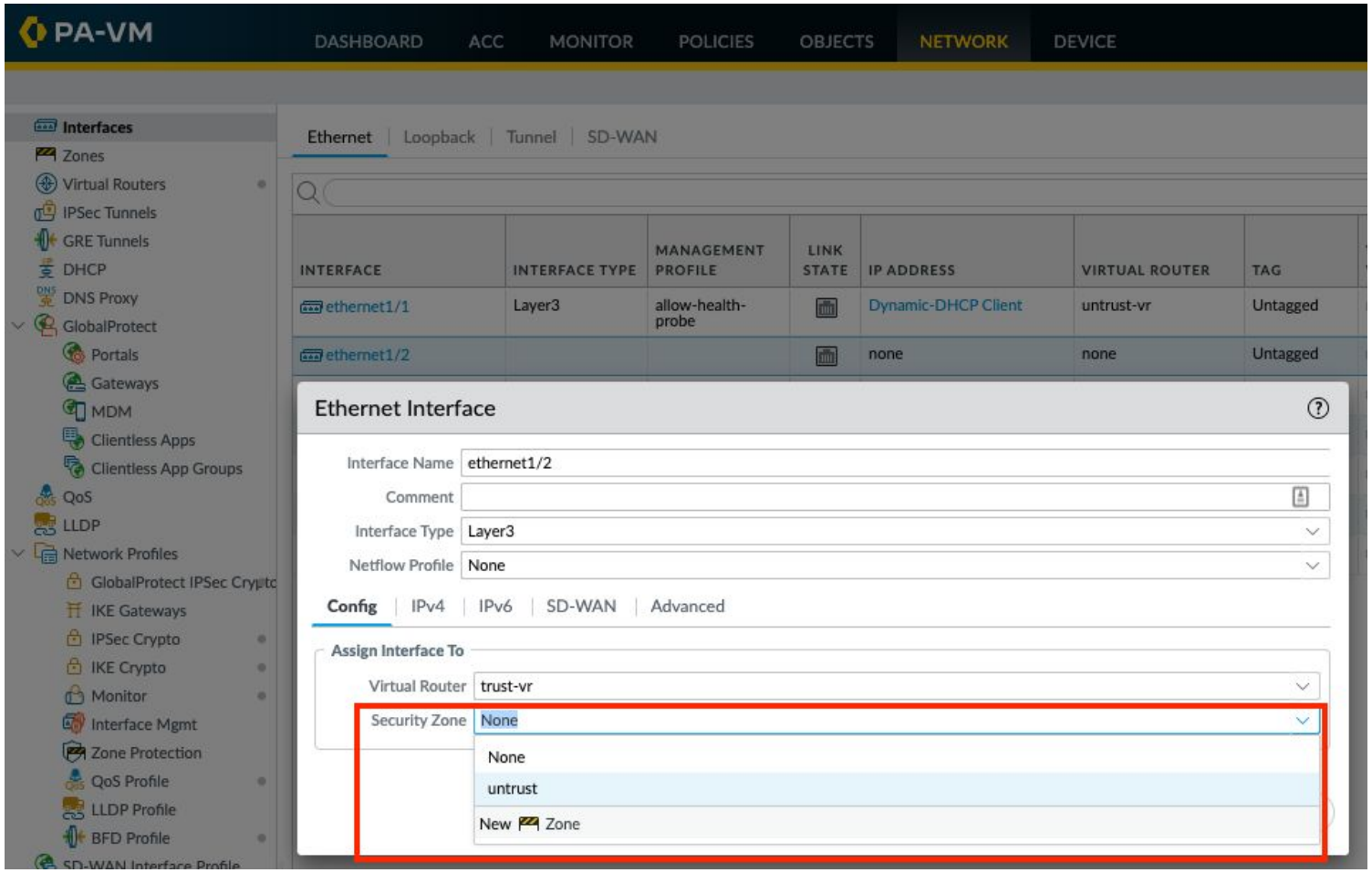
Configure Trust Interface - Virtual Router

- In the config tab select Virtual router and create a new one
- provide a proper name
- select **“ok”**



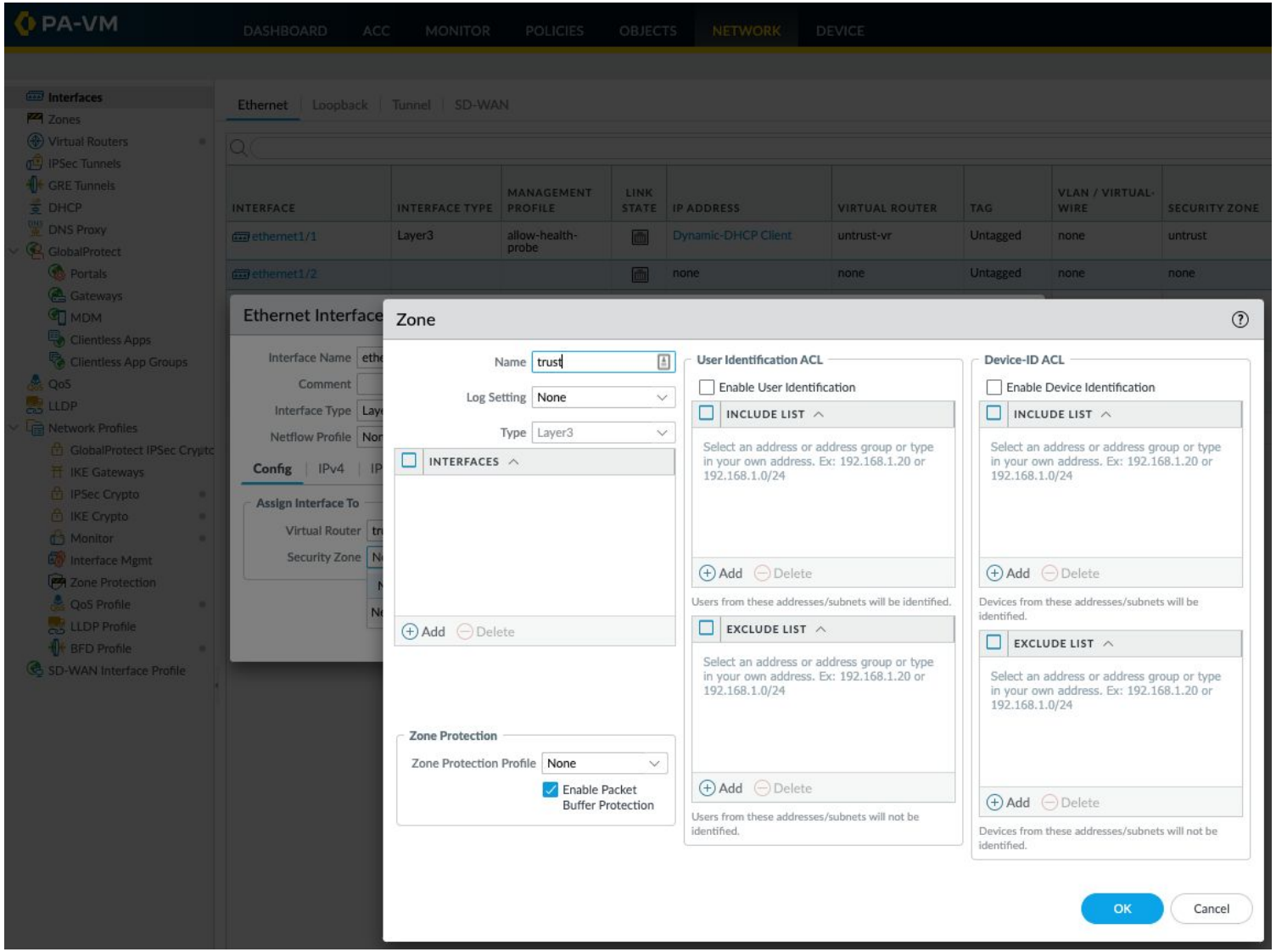
Configure Trust Interface - Zone

- In the Config tab of **“ethernet1/2”**
- Create a new zone



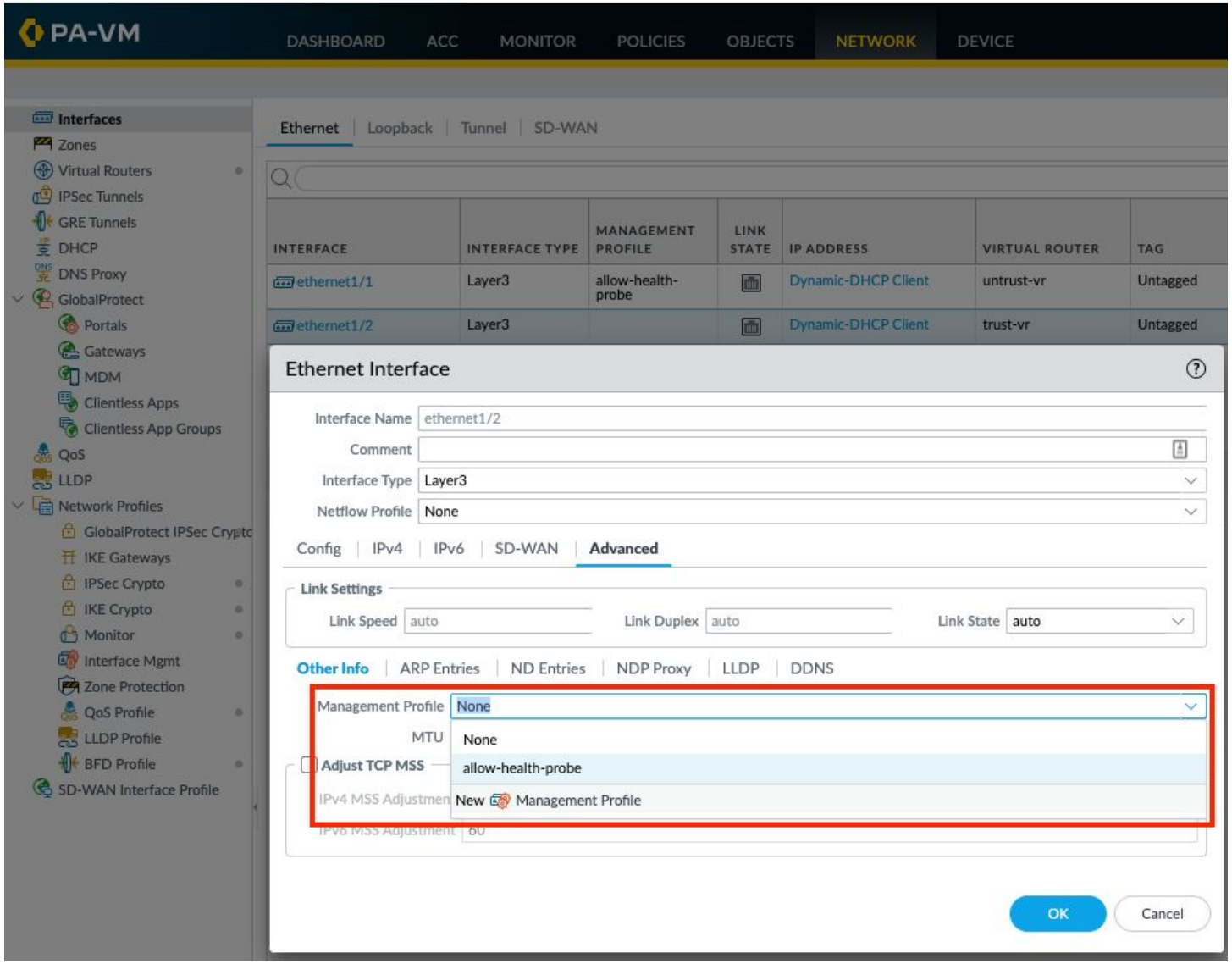
Configure Trust Interface - Zone

- provide a proper name
- select **“ok”**



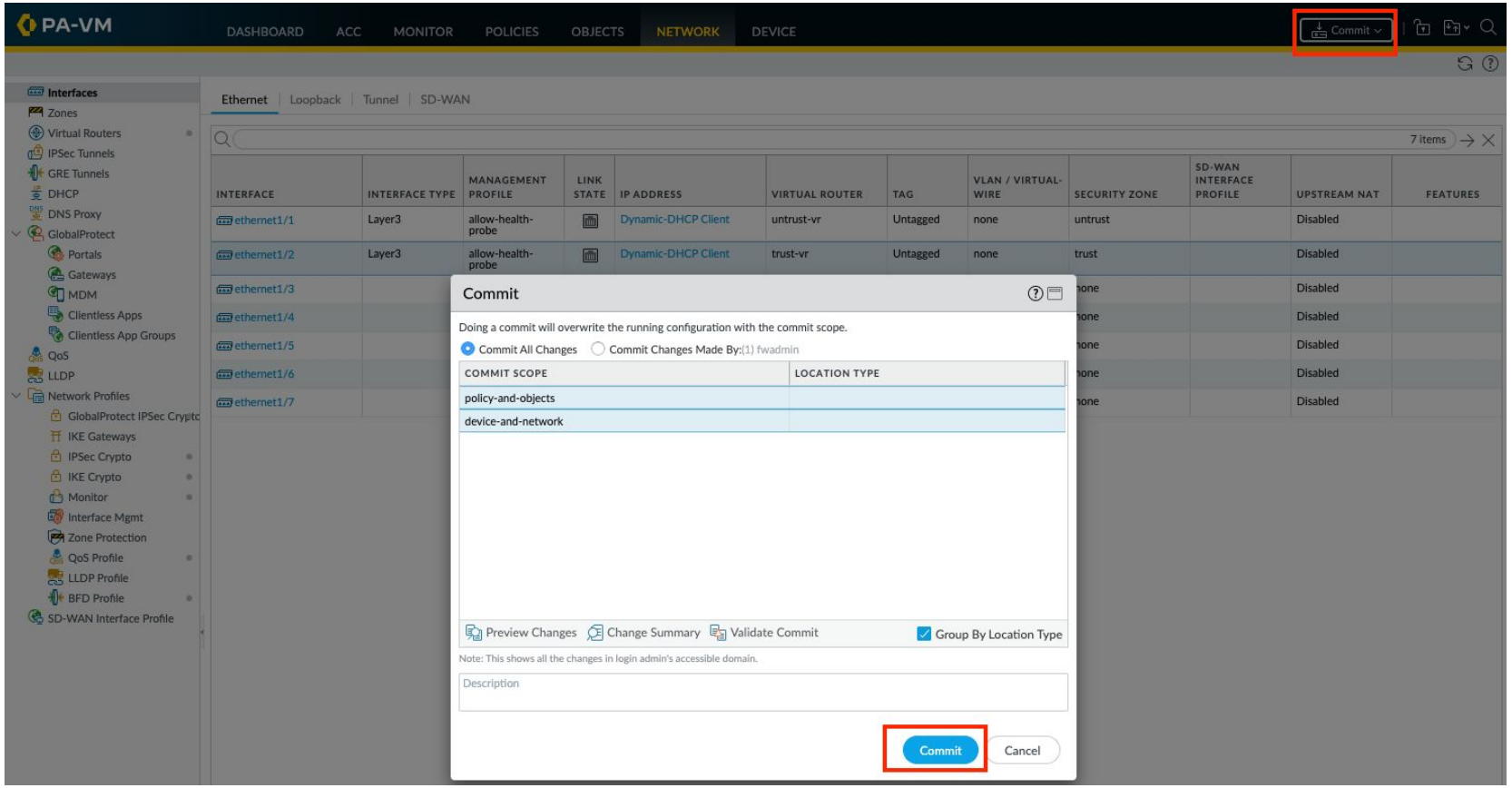
Configure Trust Interface - Advanced

- While still inside eth1/1, click Advanced Tab
- Click the Management Profile dropdown and select the previous created profile
- Click OK



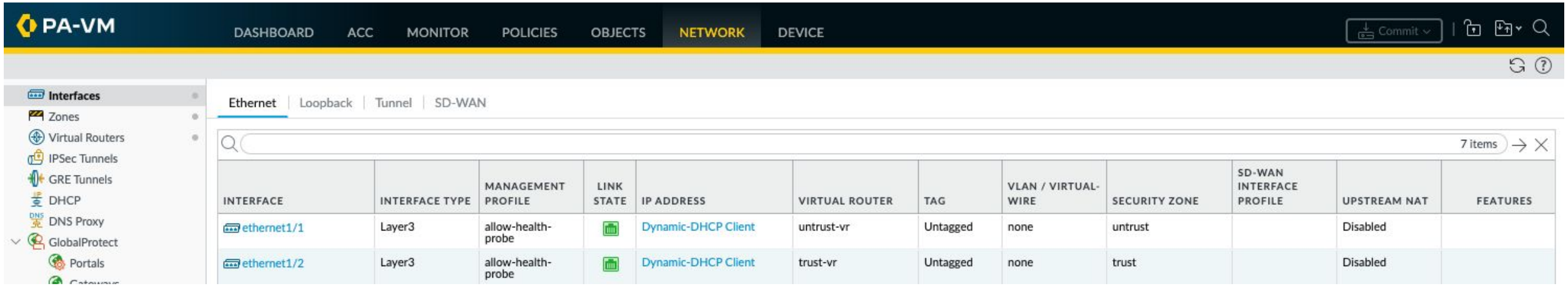
Commit your changes

- Select in the top right corner “Commit” and click again on Commit



Validate

- After the commit should your configuration looks like the picture below



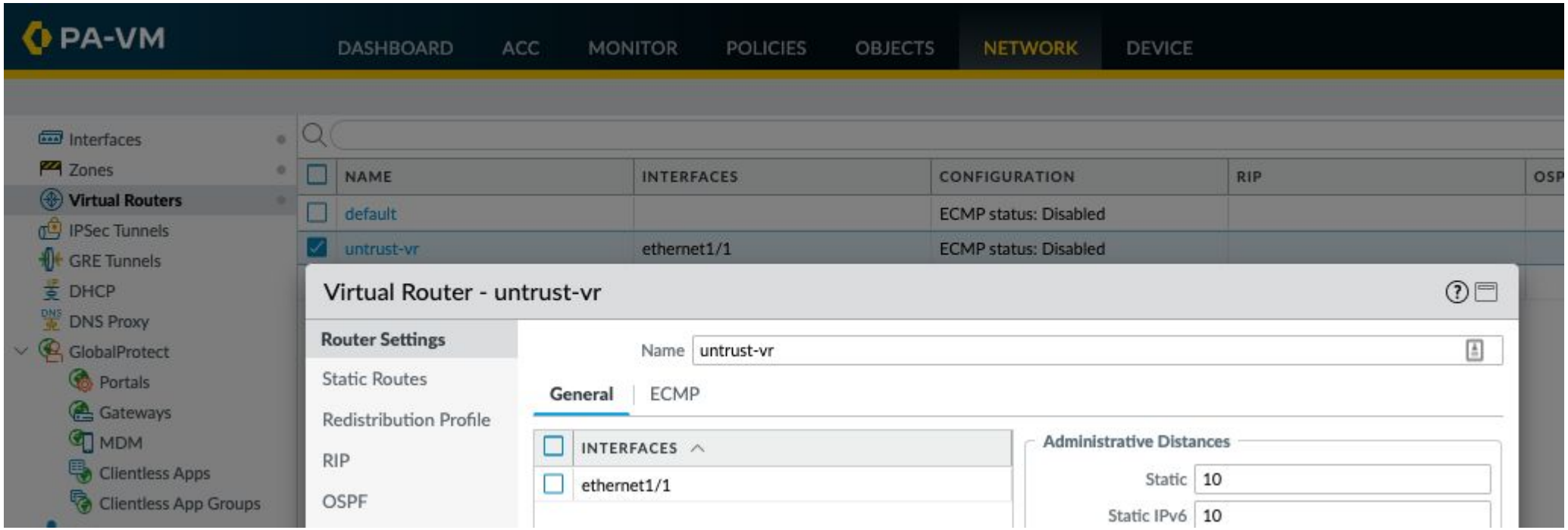
Repeat these steps on FW2 using the same settings

Configure VM-Series

Routing on Virtual Routers

Configure Untrust Virtual Router

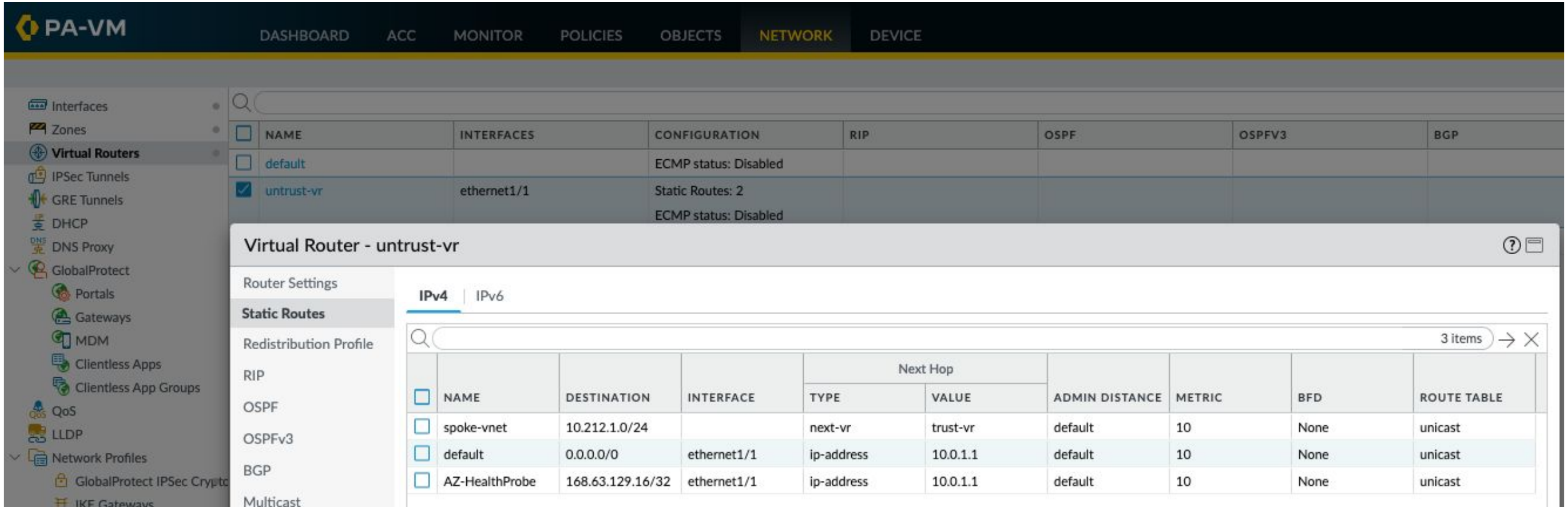
- On Slide 25 you already created the Virtual router
- On Firewall navigate to “Network”, “Virtual Router” and select the previous created “untrust-vr”



Configure Untrust Virtual Router

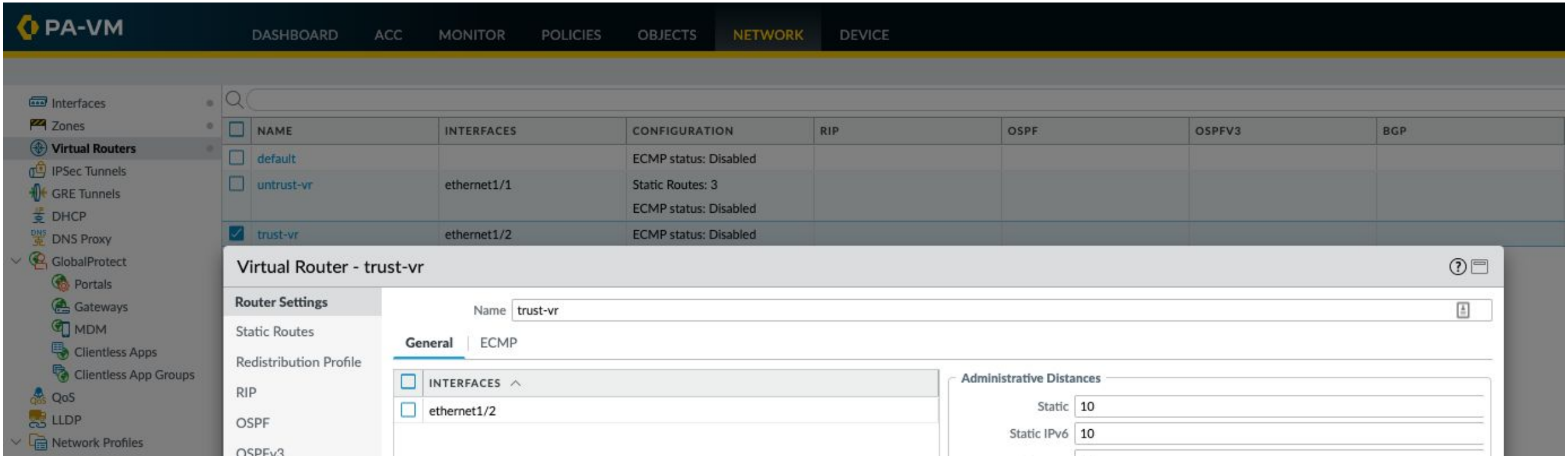
- In the Virtual Router settings of the **“untrust-vr”** select **“Static Routes”**
- Now create the following static routes as shown in the picture below

The Destination IP Addresses can be different of the spoke-vnet. Please make sure you use the same Address as you configured on the WebApp VNET



Configure Trust Virtual Router

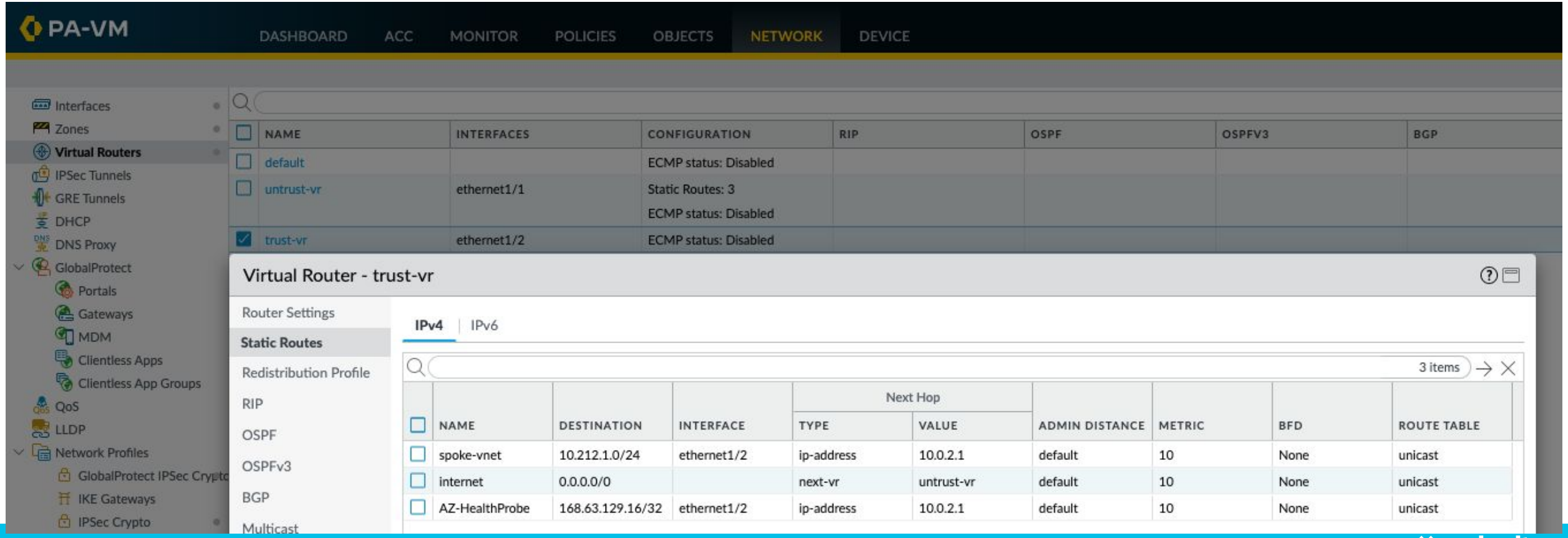
- On Slide 31 you already created the Virtual router
- On Firewall navigate to “Network”, “Virtual Router” and select the previous created “trust-vr”



Configure Trust Virtual Router

- In the Virtual Router settings of the **“trust-vr”** select **“Static Routes”**
- Now create the following static routes as shown in the picture below

The Destination IP Addresses can be different of the spoke-vnet. Please make sure you use the same Address as you configured on the WebApp VNET



COMMIT YOUR CHANGES

Repeat these steps on FW2 using the same settings

Configure VM-Series

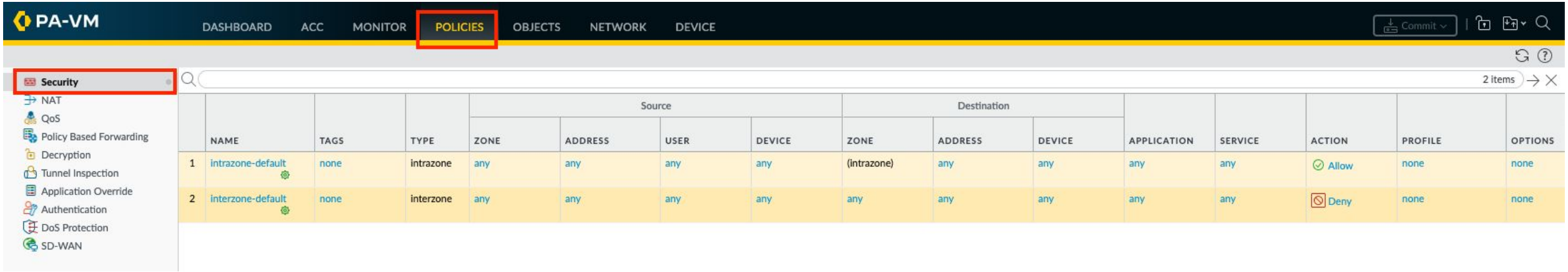
NAT & Security Policies

paloalto NETWORKS

Security Policies

Create Security Rules

- On Firewall navigate to **“Policies”**, **“Security”** and click on **“Add”** to create a new Policy

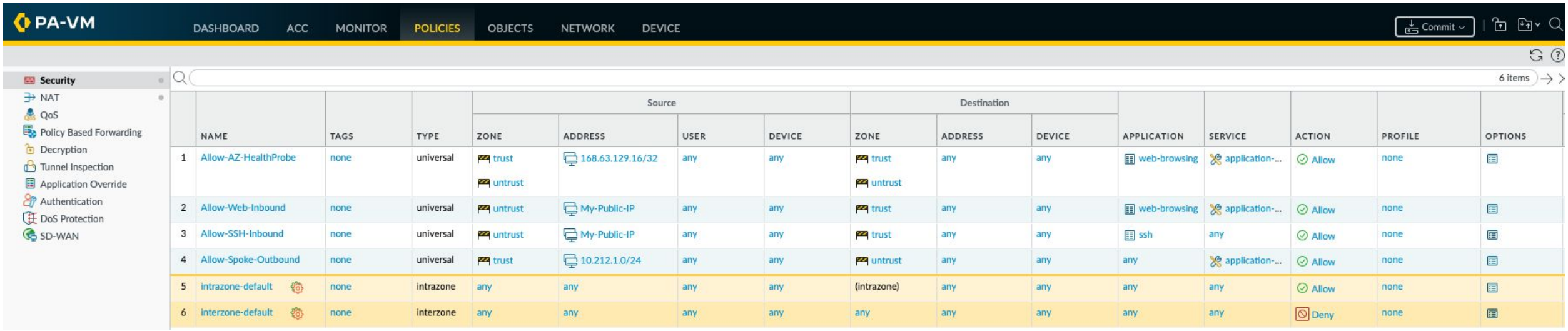


Create Security Rules

- Under the Policies, Security tab create the following Security Policies
- Please replace **“My-Public-IP”** with your Public IP

The Destination IP Addresses can be different of the spoke-vnet. Please make sure you use the same Address as you configured on the WebApp VNET

Make sure you override the “intrazone-default” and “interzone-default” to enable logging



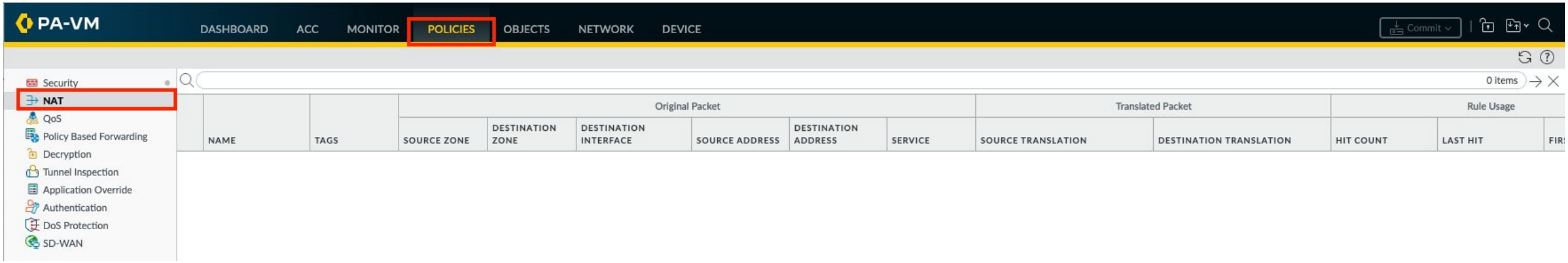
	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Allow-AZ-HealthProbe	none	universal	trust untrust	168.63.129.16/32	any	any	trust untrust	any	any	web-browsing	application-...	Allow	none	
2	Allow-Web-Inbound	none	universal	untrust	My-Public-IP	any	any	trust	any	any	web-browsing	application-...	Allow	none	
3	Allow-SSH-Inbound	none	universal	untrust	My-Public-IP	any	any	trust	any	any	ssh	any	Allow	none	
4	Allow-Spoke-Outbound	none	universal	trust	10.212.1.0/24	any	any	untrust	any	any	any	application-...	Allow	none	
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	

COMMIT YOUR CHANGES

NAT Policies

Create NAT Policies

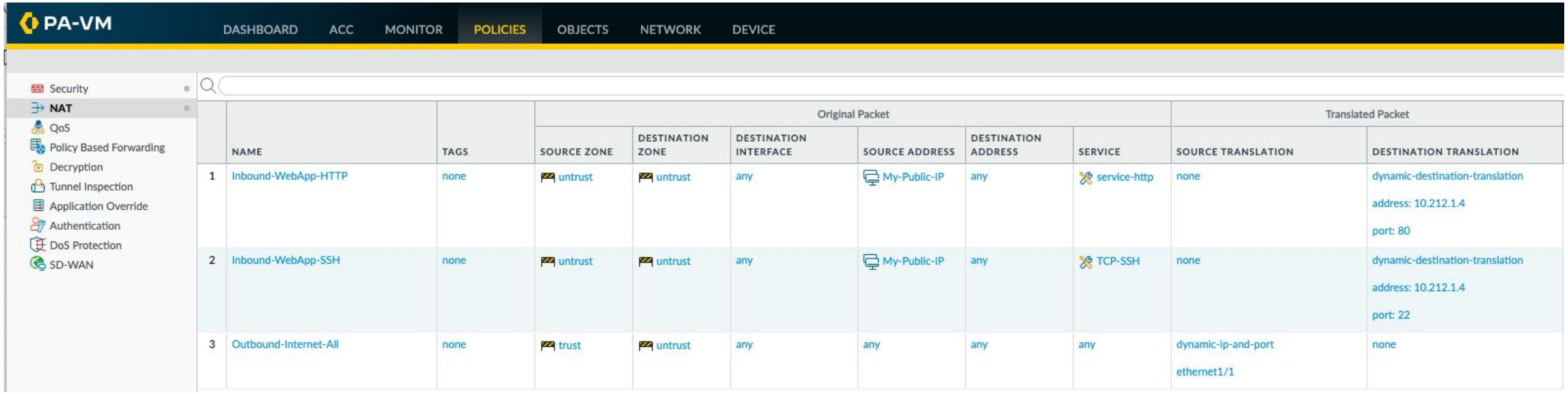
- On Firewall navigate to **“Policies”**, **“NAT”** and click on **“Add”** to create a new Policy



Create NAT Rules

- Create the following NAT Rules as shown on the picture below
- Please replace **“My-Public-IP”** with your Public IP
- The Destination IP address of the Web Server can be found here

The Destination IP Addresses can be different on the “Inbound-WebApp-HTTP” rule. Confirm that your WebApp Server has the same IP-Address



			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Inbound-WebApp-HTTP	none	untrust	untrust	any	My-Public-IP	any	service-http	none	dynamic-destination-translation address: 10.212.1.4 port: 80
2	Inbound-WebApp-SSH	none	untrust	untrust	any	My-Public-IP	any	TCP-SSH	none	dynamic-destination-translation address: 10.212.1.4 port: 22
3	Outbound-Internet-All	none	trust	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

COMMIT YOUR CHANGES

Repeat these steps on FW2 using the same settings

Configure WebApp Resource Group

Next Steps

1. **Create Virtual Network Peerings** between the newly deployed “Hub” and any applications Virtual Networks.
2. **Create a Route Table** in the Application Virtual Networks to forward traffic to the “Egress Private IP” which is the Private IP of the Internal Load Balancer.
    - For instance “0.0.0.0/0” to “Egress Private IP” for Outbound / East-West Traffic
3. **Configure Web-App Server** to simulate a Web Server
    - Upgrade OS
    - Install Apache Web Server

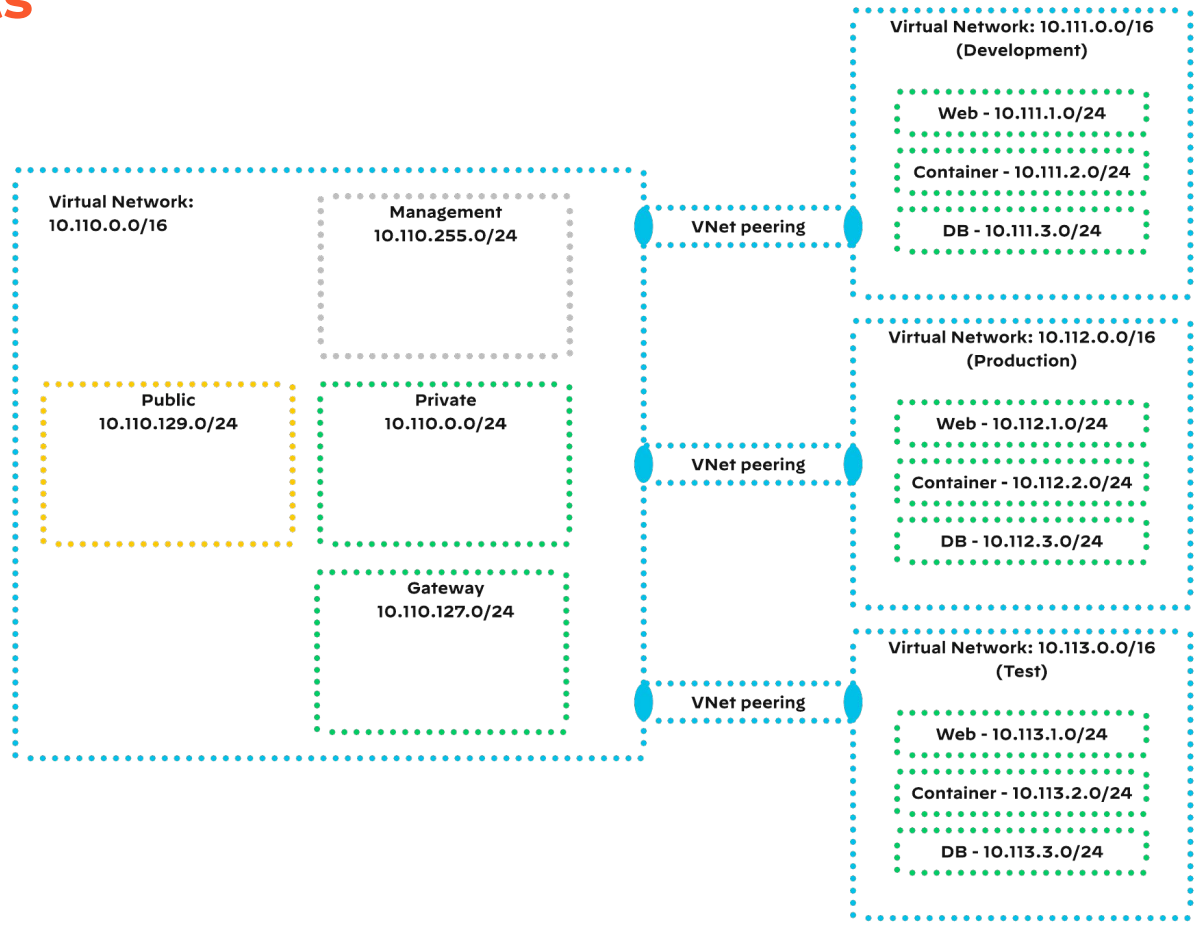
Configure WebApp Resource Group

Create VNet Peering

What is VNet Peering?

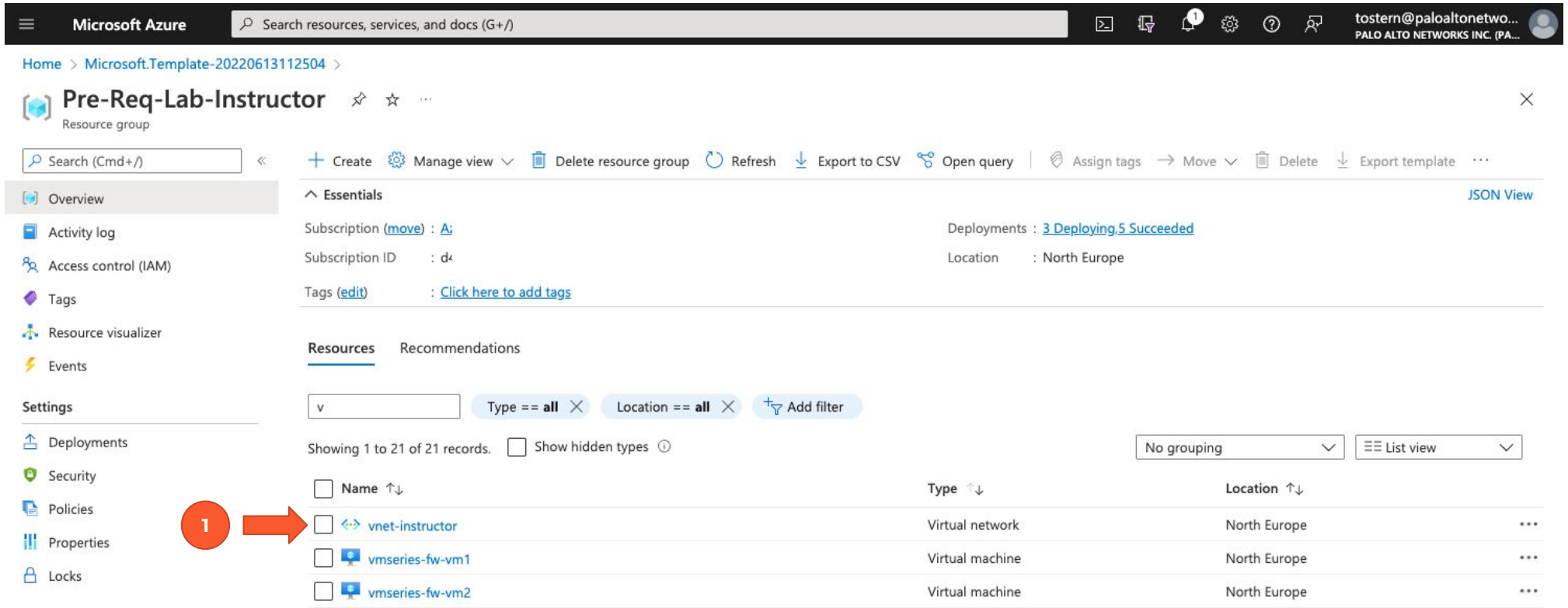
Full seamless IP reachability across VNets

- VNets can be connected as long as there is no overlap in the IP network definition.
- All network traffic remains within the Azure backbone.



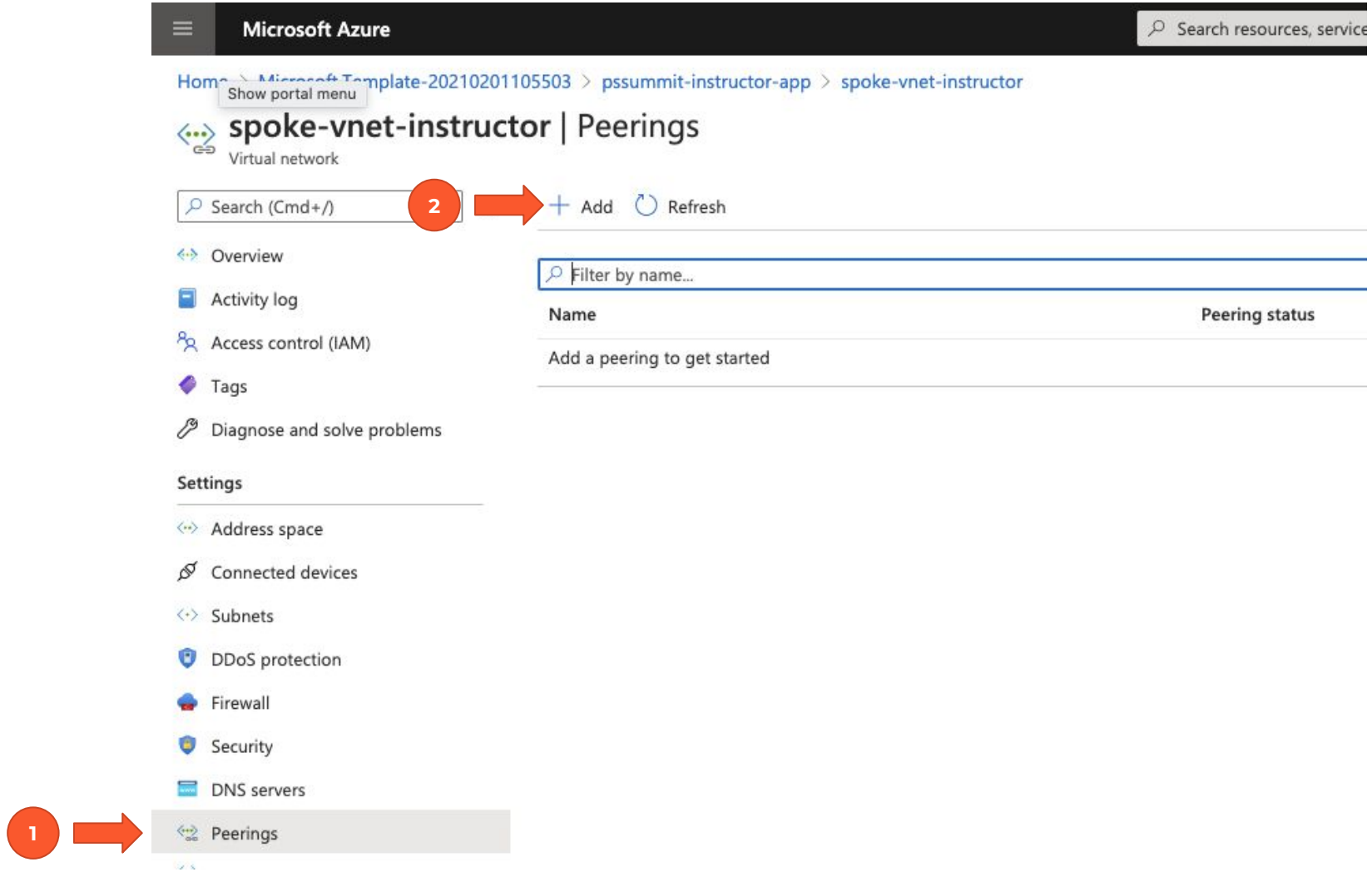
Create VNET peering

- Select the Virtual Network in the Resource Group you created on here
  - Example “vnet-instructor”



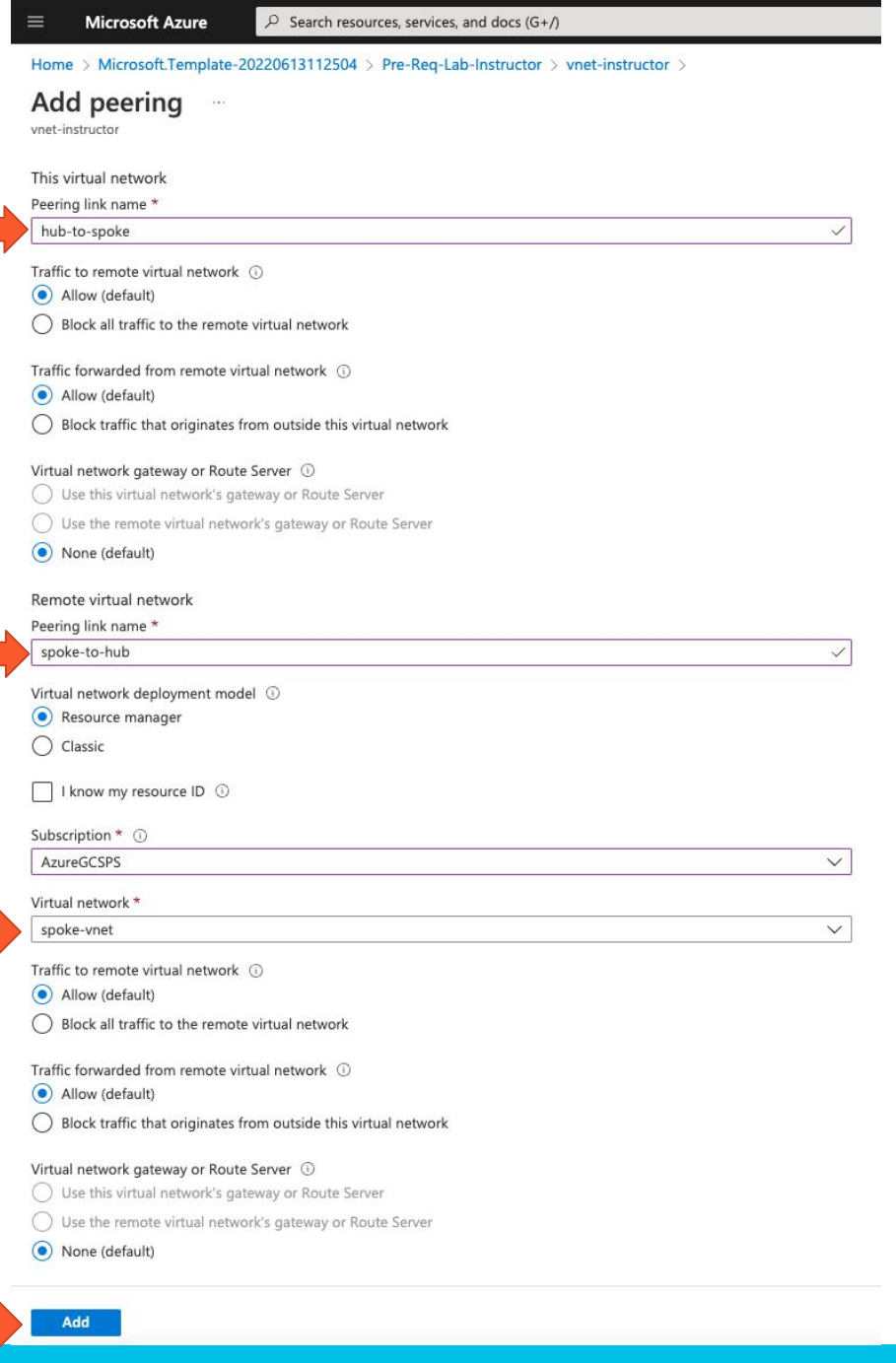
Create VNET peering

- Select **“Peerings”**
- Click **“Add”**



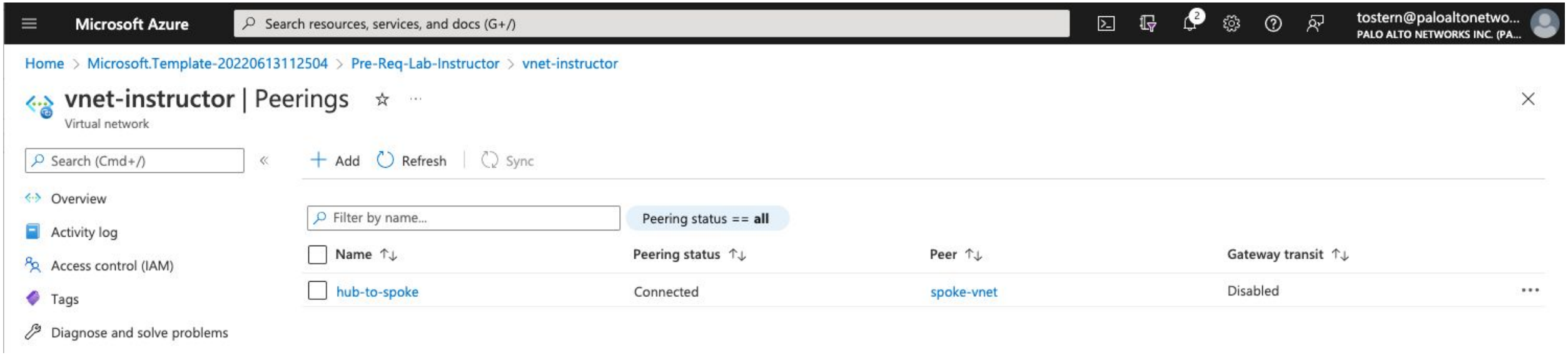
Create VNET peering

1. Use the same name
2. Use the same name
3. Select here the VNET that you created on Slide 16
4. Select Add



Validate VNET peering

When the peering was successful you should see the following the Azure Dashboard under Peerings



Configure WebApp Resource Group

Create/Configure Route Table

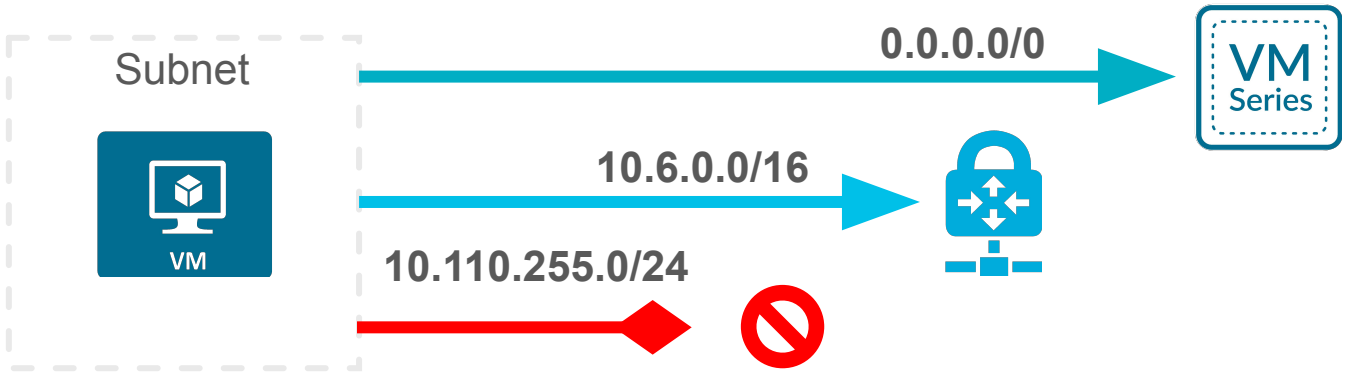
What is a Route Table/User defined Route?

Modify the default traffic forwarding behavior of Azure networking

- Associated to subnets and applies to traffic that is leaving the subnet.
- The destination for a route can be a different subnet in the VNet, anywhere on the Internet, or a private network connected to the VNet.

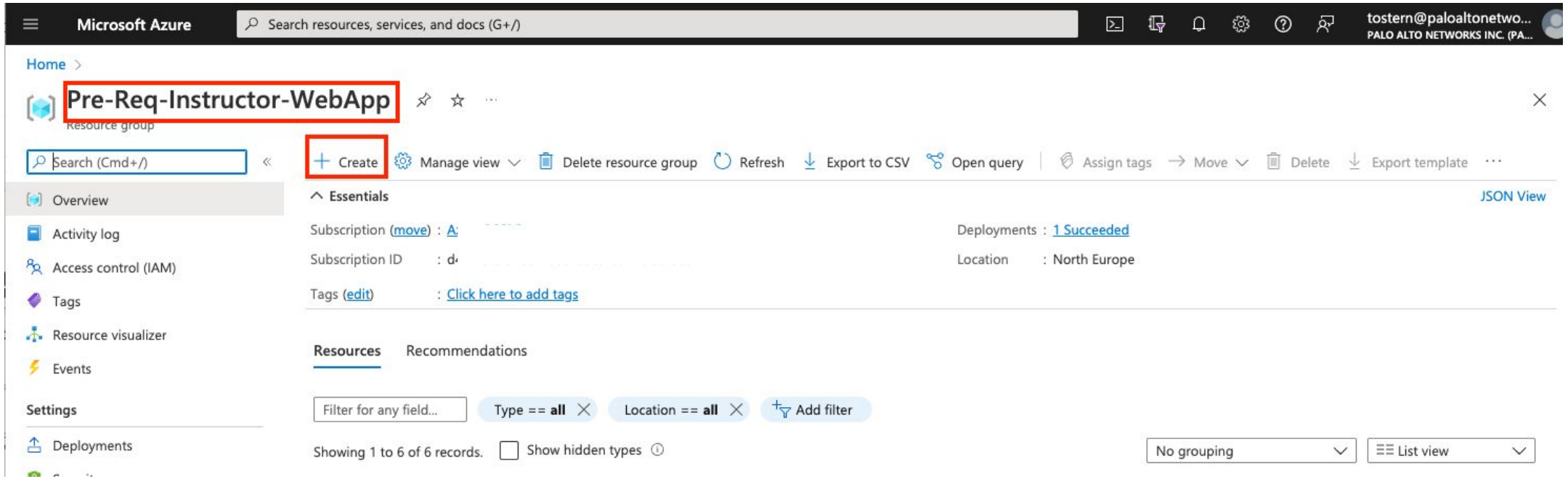
The next-hop for the route can be

- The VNet or peered VNet (default)
- Internet
- A virtual machine in the VNet
- VPN/ExpressRoute connection
- Blackhole traffic (None)



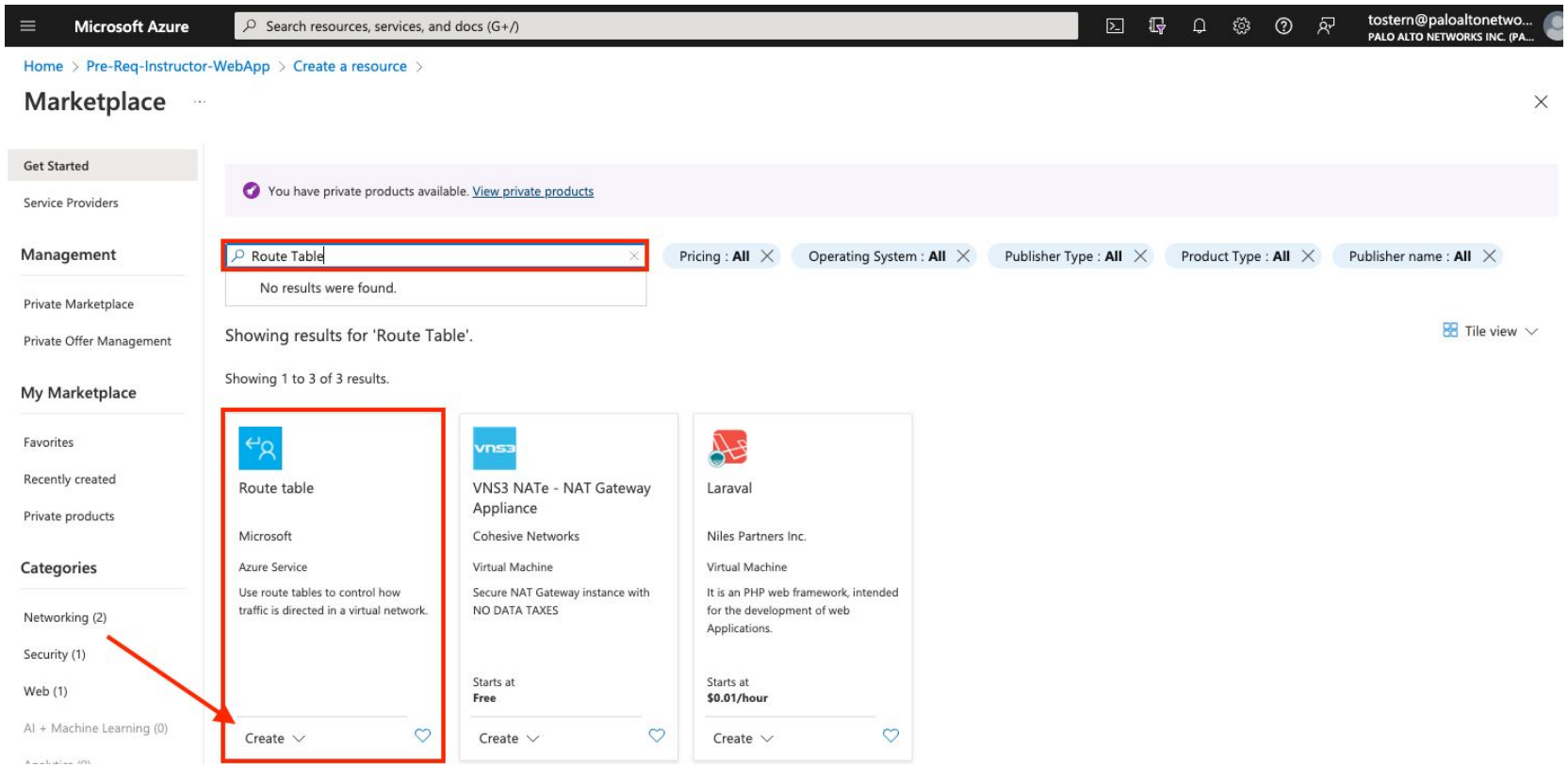
Create Route table

1. Go to your WebApp Resource Group
2. Click von “Create



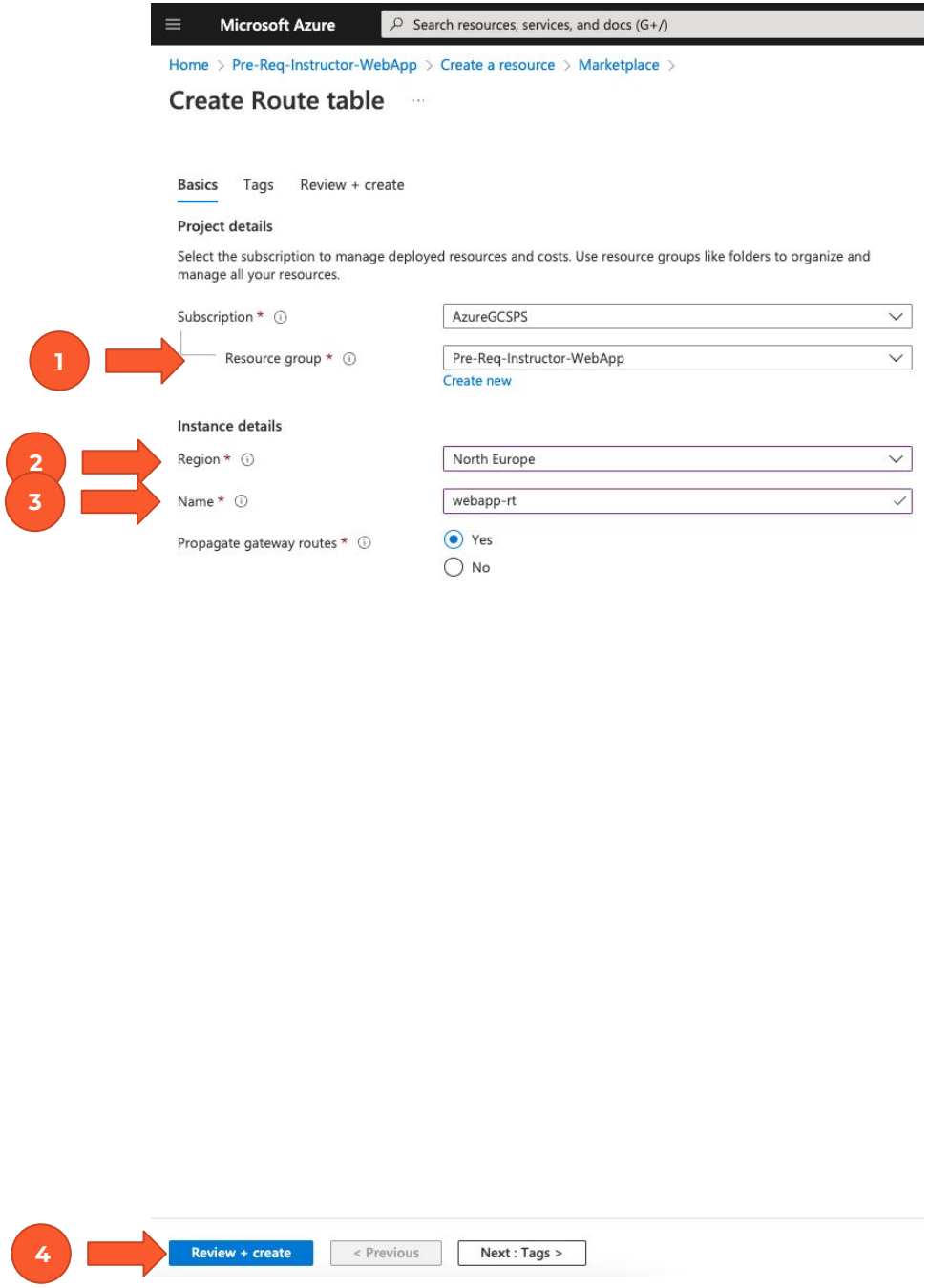
Create Route table

1. Type in the Search field “Route Table”
2. Click von “Create” in the “Route Table”



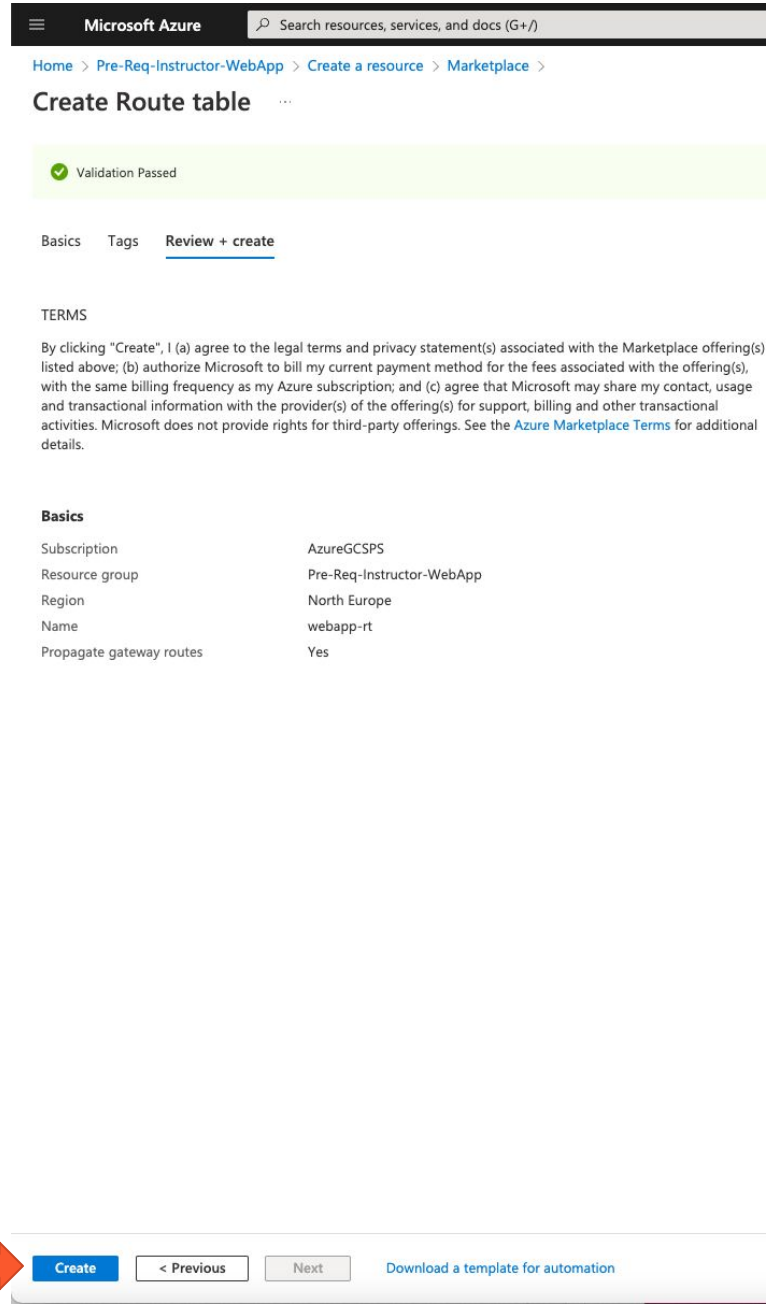
Create Web-App Route table

1. Make sure your WebApp RG is selected
2. Change it to your region
3. Give it a proper name
4. Click “Review+Create



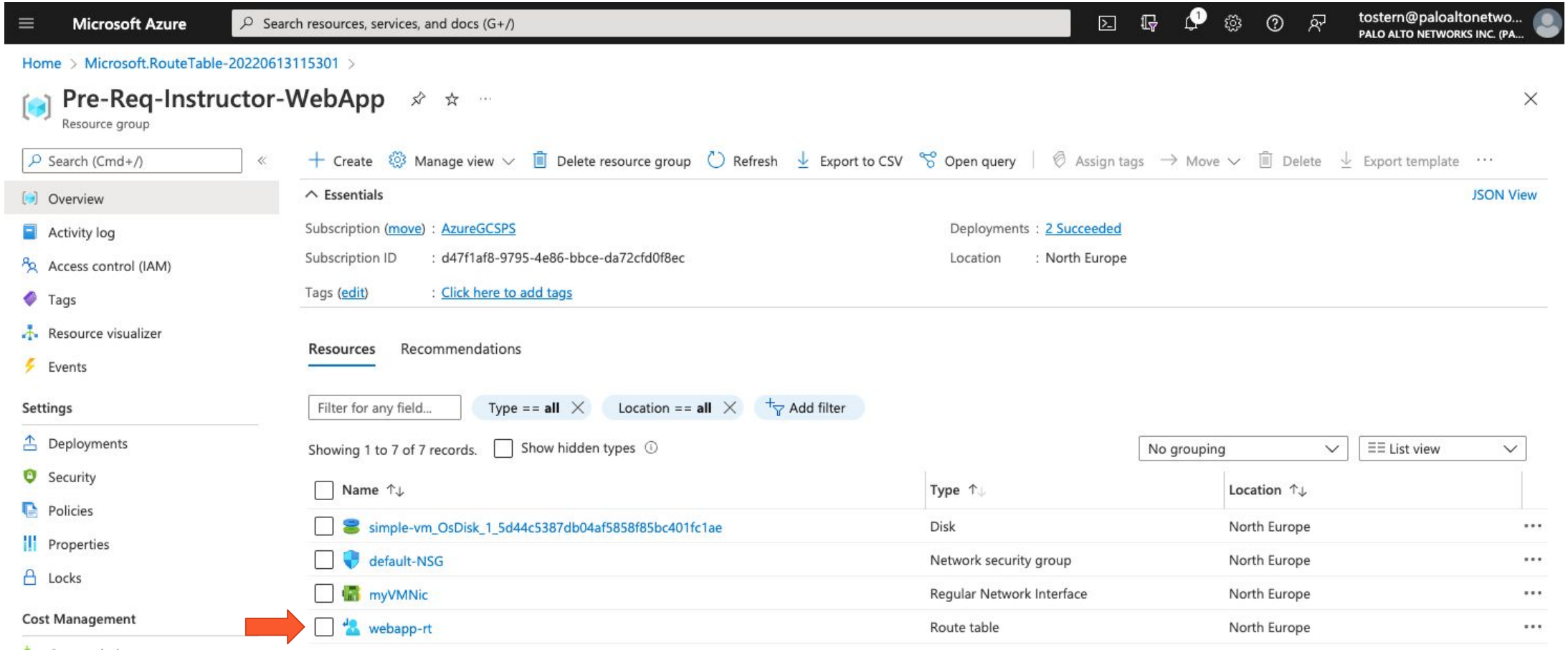
Create Web-App Route table

1. Select Create after the validation passed



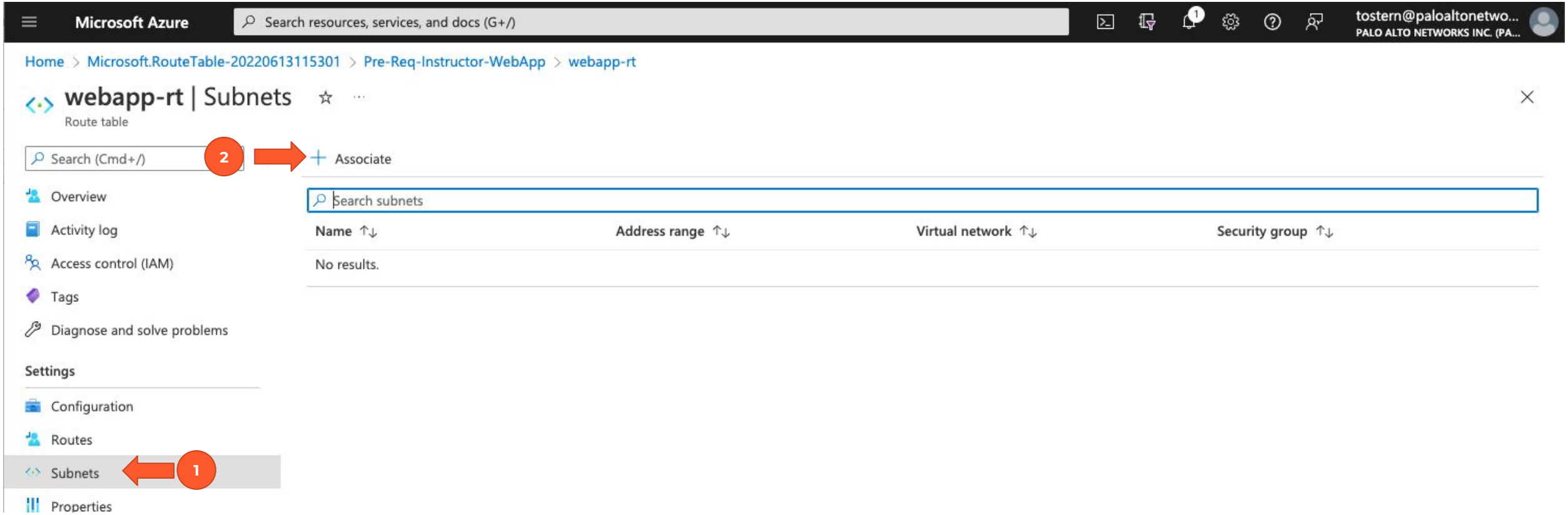
Configure Route Table

- Select the previous create route table in your WebApp Resource Group



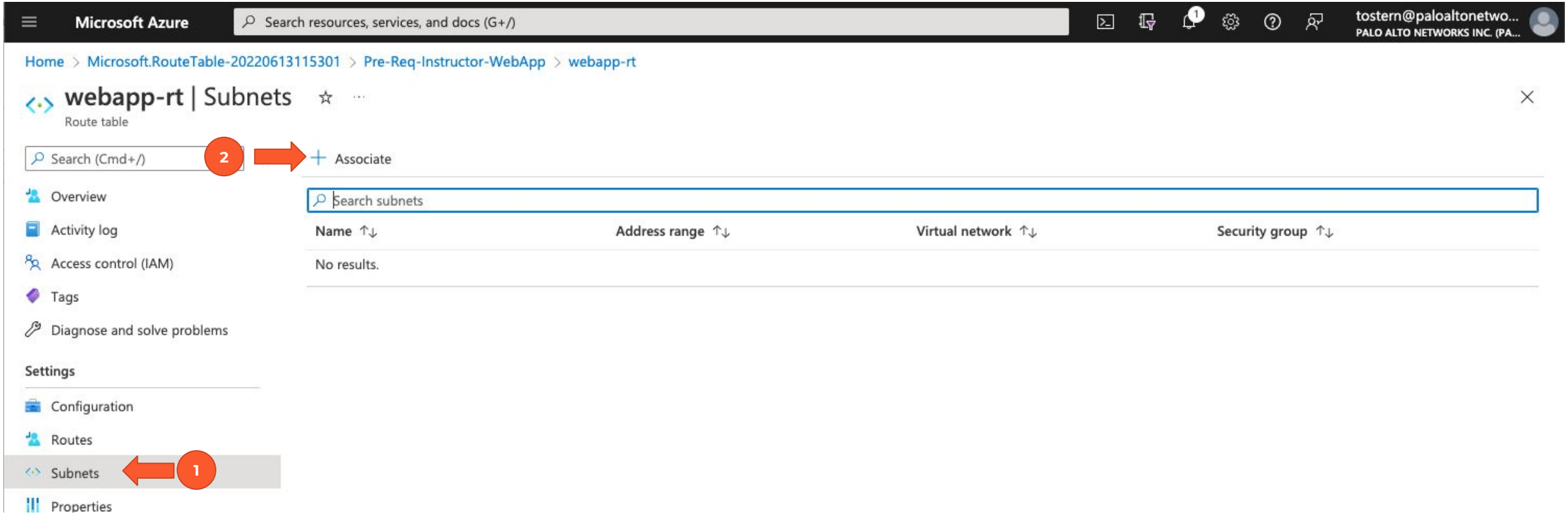
Associate Route table with a subnet

1. Select **Subnets**
2. Click **Associate**



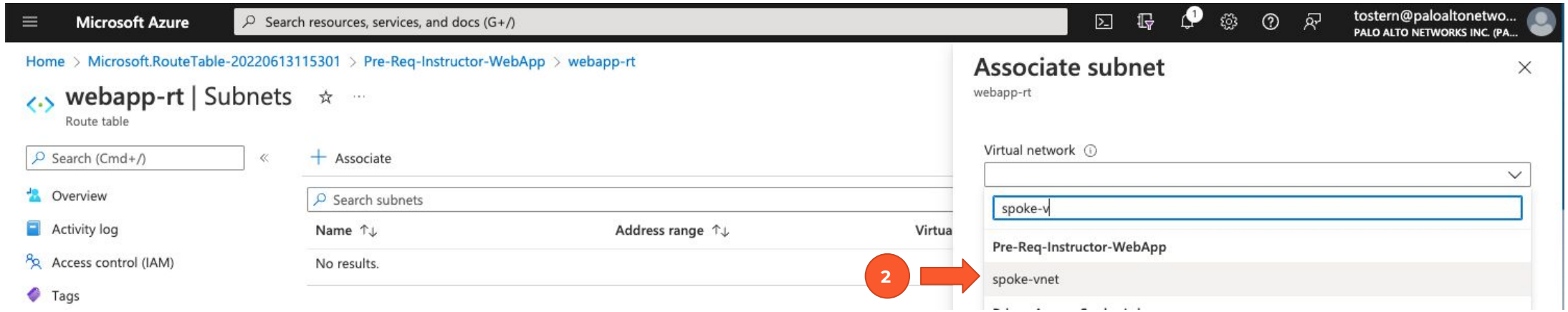
Associate Route table with a subnet

1. Select **Subnets**
2. Click **Associate**



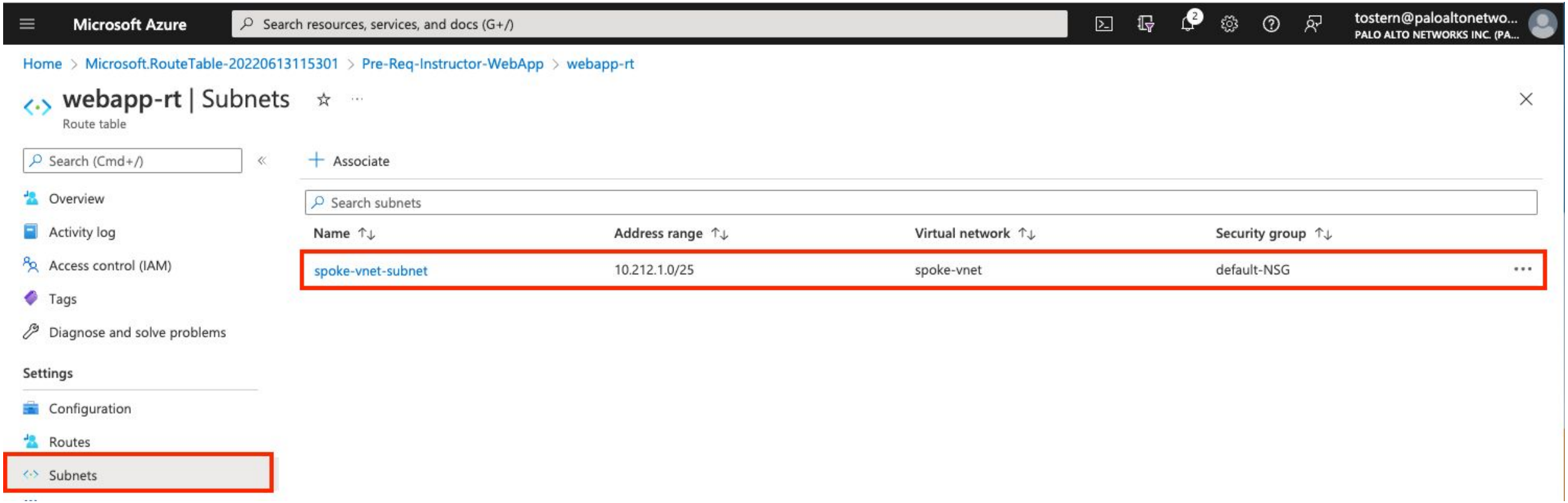
Associate Route table with a subnet

1. Select under Virtual Network your Virtual Network of the WebApp Resource Group
2. Select the Subnet you get listed
3. Click OK



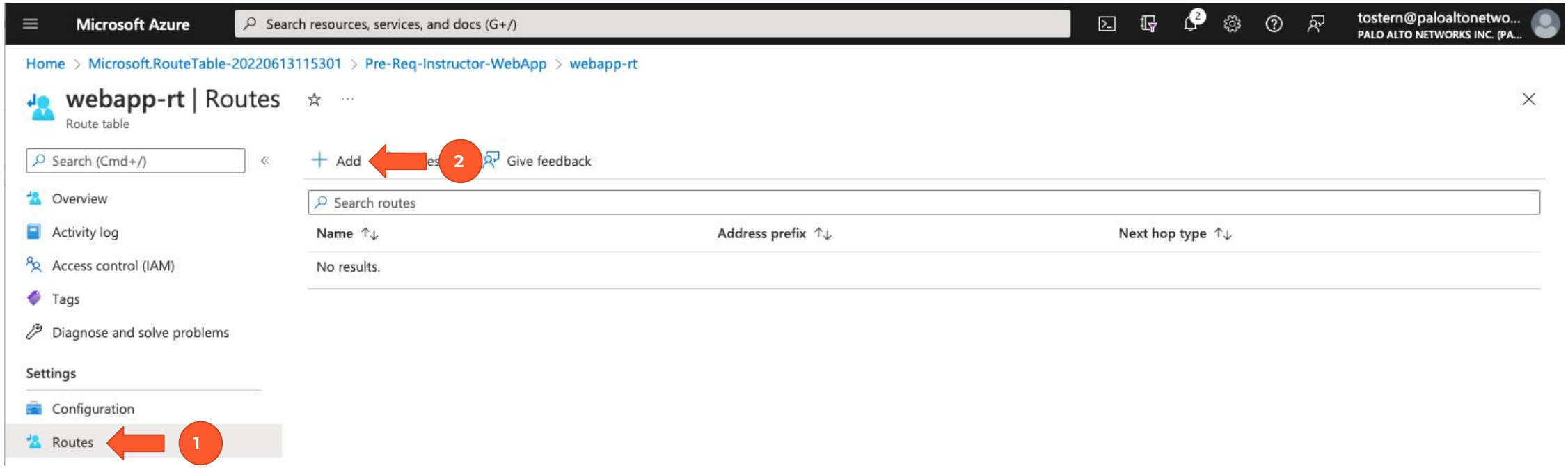
Associate Route table with a subnet

- Validate that subnet is listed under **“Subnets”**



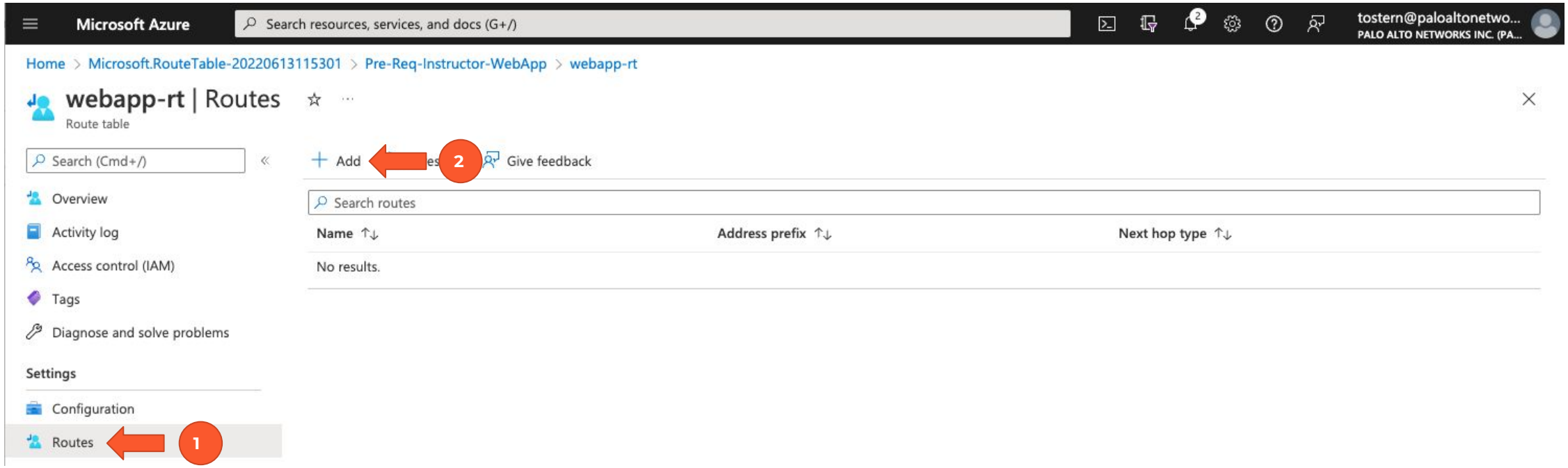
Create static Route

1. In the created **“webapp-rt”** select **“Routes”**
2. Select **“Add”**



Create static Route

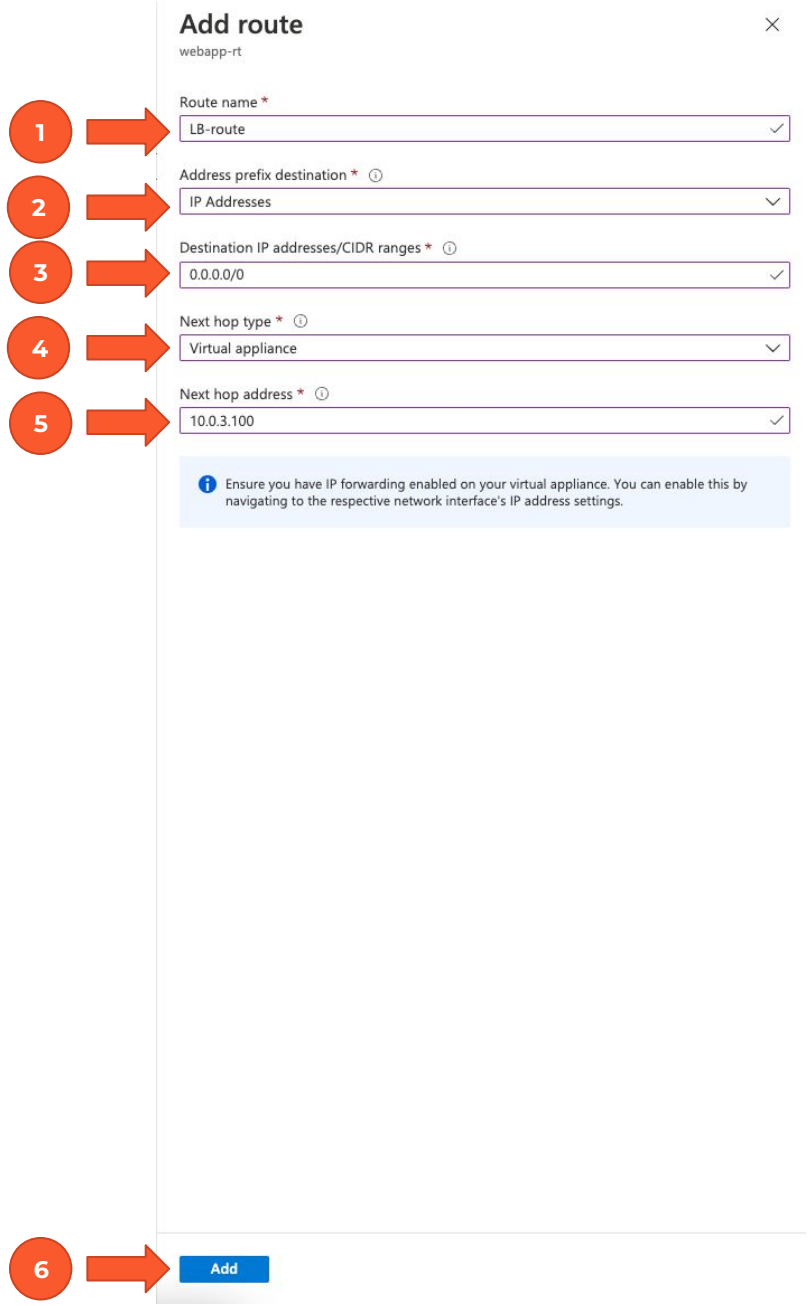
1. In the created **“webapp-rt”** select **“Routes”**
2. Select **“Add”**



Create static Route

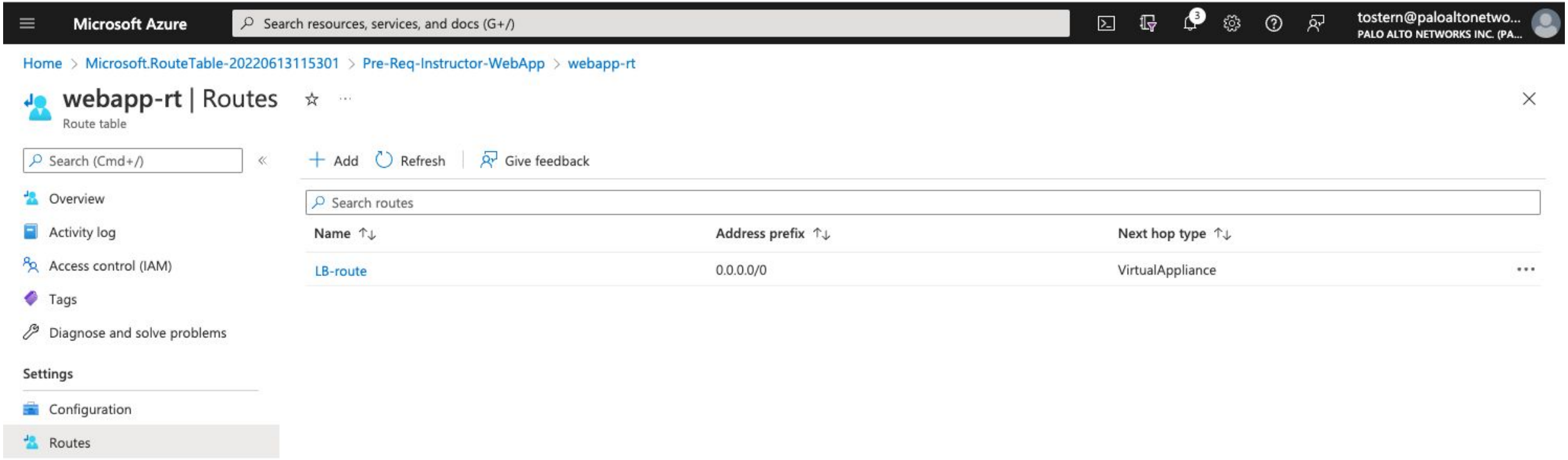
1. Give it a proper name
2. Select IP Addresses
3. Address prefix: 0.0.0.0/0
4. Next hop type: Virtual Appliance
5. Next hop address: Private Frontend IP of the Hub Internal Load Balancer (Here can find the IP)
6. Select Add

It can take up to 5 minutes that the added route are effective in the Azure route table



Validate static Route

- Validate that the created route is listed under **“Routes”**

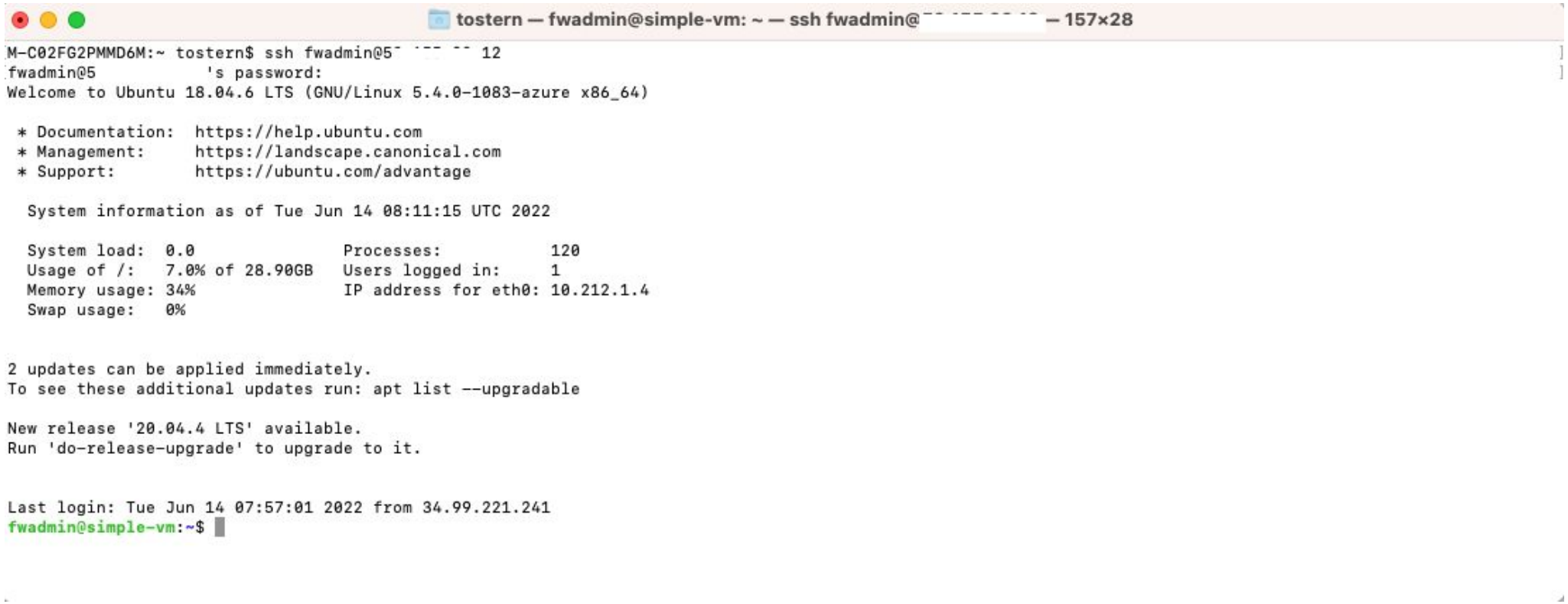


Configure Web Server

Configure Web Server

Login into Web Server

- Login into the Web Server via the SSH
  - **ssh <username>@<PublicIPLoadBalancer>**
  - See Slide how to find the Public IP of the Public Load Balancer
  - use the username you configured here



Update Web Server

- Upadte Web Server by using the following command
  a. **sudo apt-get update**

```
[fwadmin@simple-vm:~$
[fwadmin@simple-vm:~$
[fwadmin@simple-vm:~$ sudo apt-get update
Hit:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic/universe amd64 Packages [8570 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic/universe Translation-en [4941 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse amd64 Packages [151 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en [108 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [2621 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1821 kB]
Get:11 http://azure.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [395 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packages [24.9 kB]
Get:13 http://azure.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation-en [6012 B]
Get:14 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main amd64 Packages [10.8 kB]
Get:15 http://azure.archive.ubuntu.com/ubuntu bionic-backports/main Translation-en [5016 B]
Get:16 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packages [11.6 kB]
Get:17 http://azure.archive.ubuntu.com/ubuntu bionic-backports/universe Translation-en [5864 B]
Get:18 http://azure.archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [2279 kB]
Get:19 http://azure.archive.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [1209 kB]
Get:20 http://azure.archive.ubuntu.com/ubuntu bionic-security/universe Translation-en [279 kB]
Get:21 http://azure.archive.ubuntu.com/ubuntu bionic-security/multiverse amd64 Packages [19.0 kB]
Get:22 http://azure.archive.ubuntu.com/ubuntu bionic-security/multiverse Translation-en [3836 B]
Fetched 22.7 MB in 4s (5466 kB/s)
Reading package lists... Done
```

Install Web Server

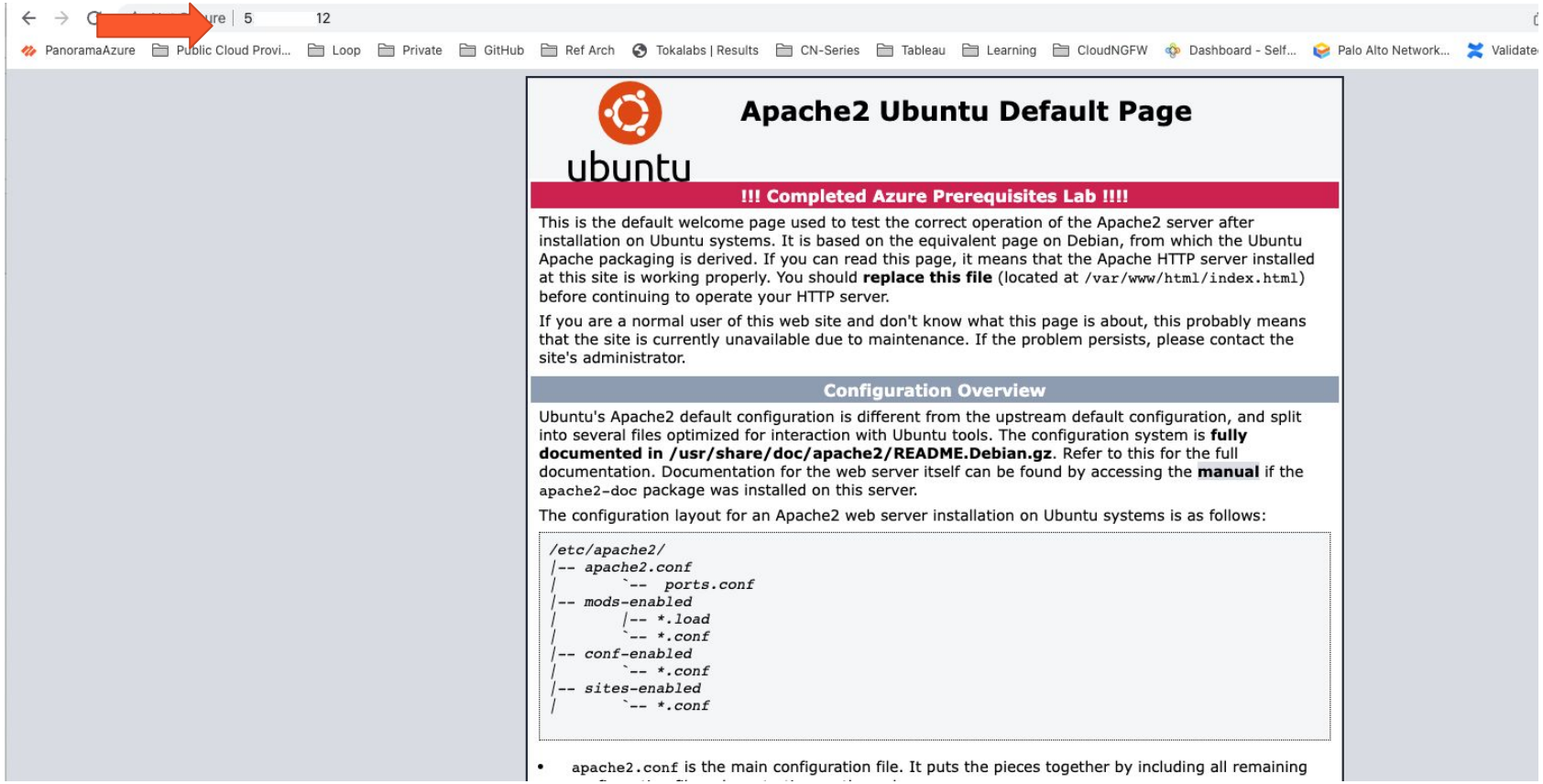
- Install Apache Web Server on the VM
  a. **sudo apt-get install apache2 -y**

```
fwadmin@simple-vm:~$ sudo apt-get install apache2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 2 not upgraded.
Need to get 1730 kB of archives.
After this operation, 6997 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 libapr1 amd64 1.6.3-2 [90.9 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1 amd64 1.6.1-2 [84.4 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-2 [10.6 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1-ldap amd64 1.6.1-2 [8764 B]
Get:5 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 liblua5.2-0 amd64 5.2.4-1.1build1 [108 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-bin amd64 2.4.29-1ubuntu4.23 [1071 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-utils amd64 2.4.29-1ubuntu4.23 [84.1 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2-data all 2.4.29-1ubuntu4.23 [160 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu bionic-updates/main amd64 apache2 amd64 2.4.29-1ubuntu4.23 [95.1 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu bionic/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Fetched 1730 kB in 0s (5004 kB/s)
```

Test Traffic flow

Connect to Web Server

- Type in your browser the Frontend IP of your Public Load Balancer (http://<PIP-LB>)
- You can find the IP here



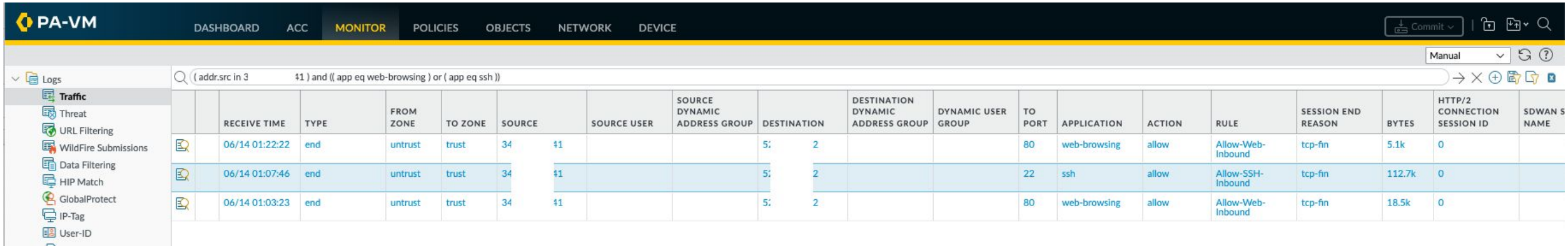
Validate Outbound Traffic in your logs

- use the following filter to find the outbound logs **“(addr.src in 10.212.1.4) and (app eq apt-get)”**
- You should see the “apt-get” request in your logs

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN S NAME
		06/14 01:06:26	end	trust	untrust	10.212.1.4			51.104.174.161			80	apt-get	allow	Allow-Spoke-Outbound	tcp-fin	3.2k	0	
		06/14 01:02:44	end	trust	untrust	10.212.1.4			51.104.174.161			80	apt-get	allow	Allow-Spoke-Outbound	tcp-fin	1.8M	0	
		06/14 01:02:25	end	trust	untrust	10.212.1.4			51.104.174.161			80	apt-get	allow	Allow-Spoke-Outbound	tcp-fin	23.8M	0	

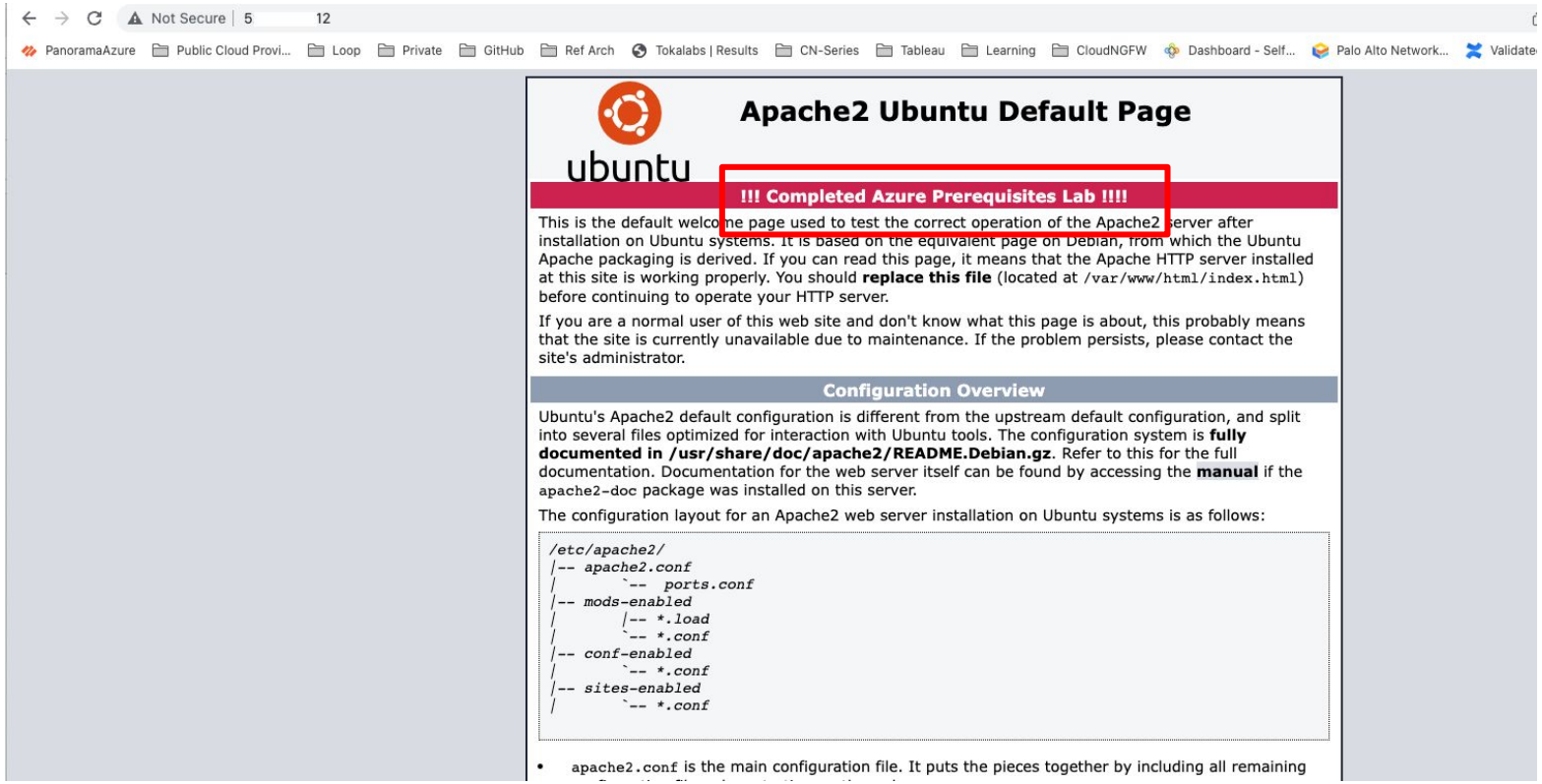
Validate Inbound Traffic in your logs

- use the following filter to find the outbound logs **“(addr.src in <your public ip>) and ((app eq web-browsing) or (app eq ssh))”**
- You should see the following request in your logs



Change Web Server default page

- Change default page
  - https://askubuntu.com/questions/857609/apache2-now-pointing-to-new-default-page



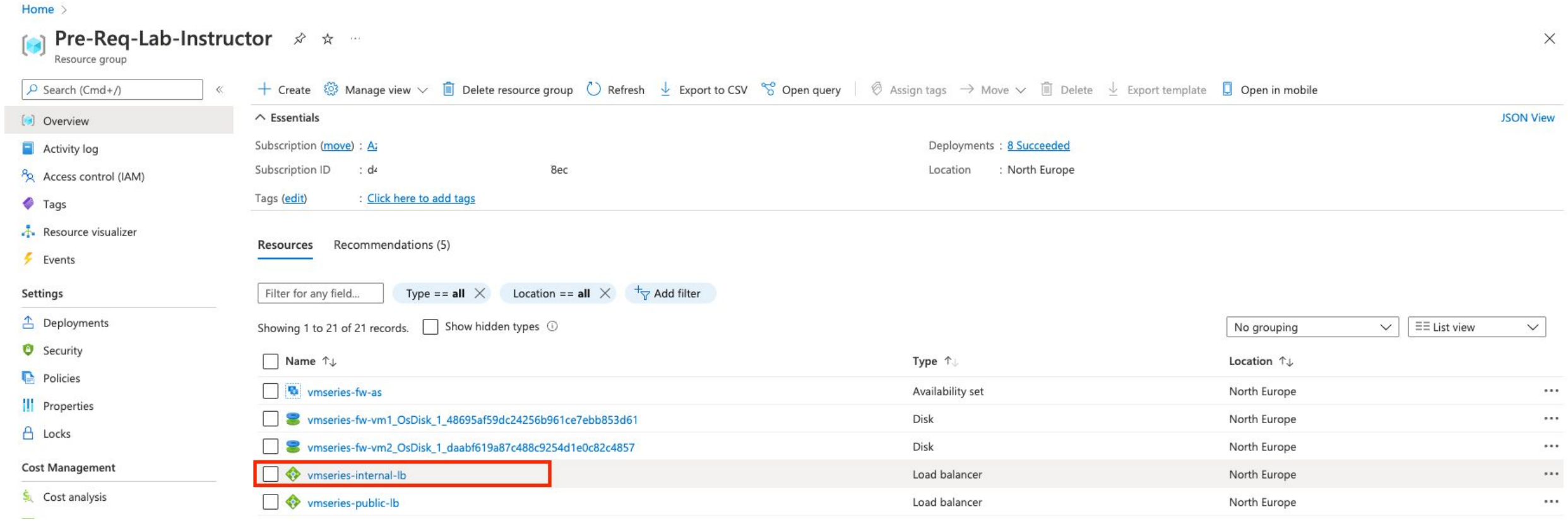
paloalto NETWORKS

Thank you

Backup Slides

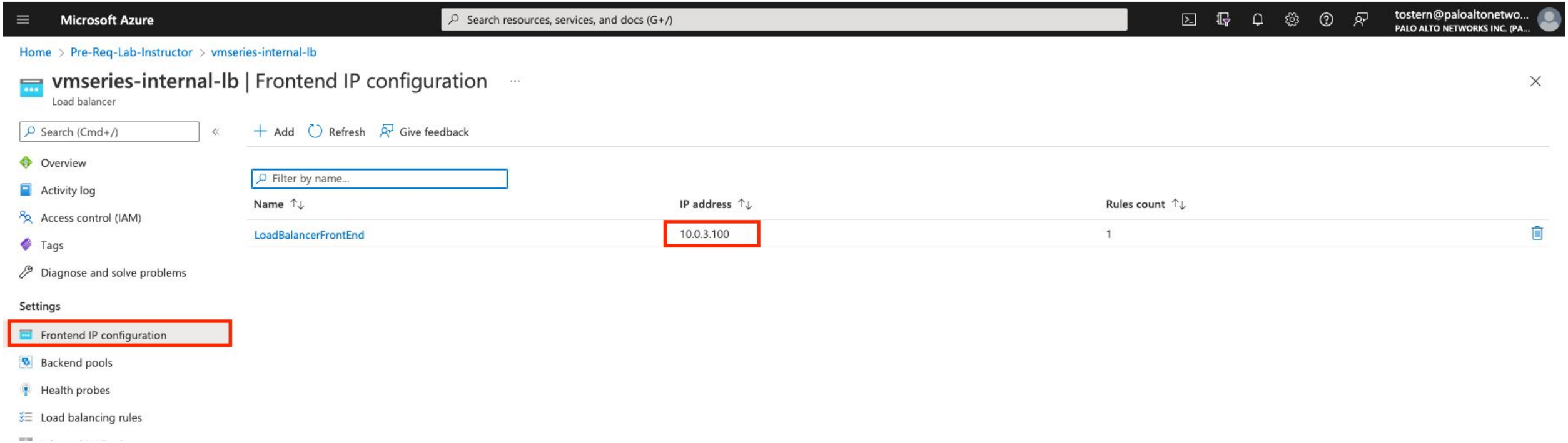
How to find Frontend IP addresses of Internal Load Balancer?

- Navigate to your resource group you created here and select the **“vmseries-internal-lb”**



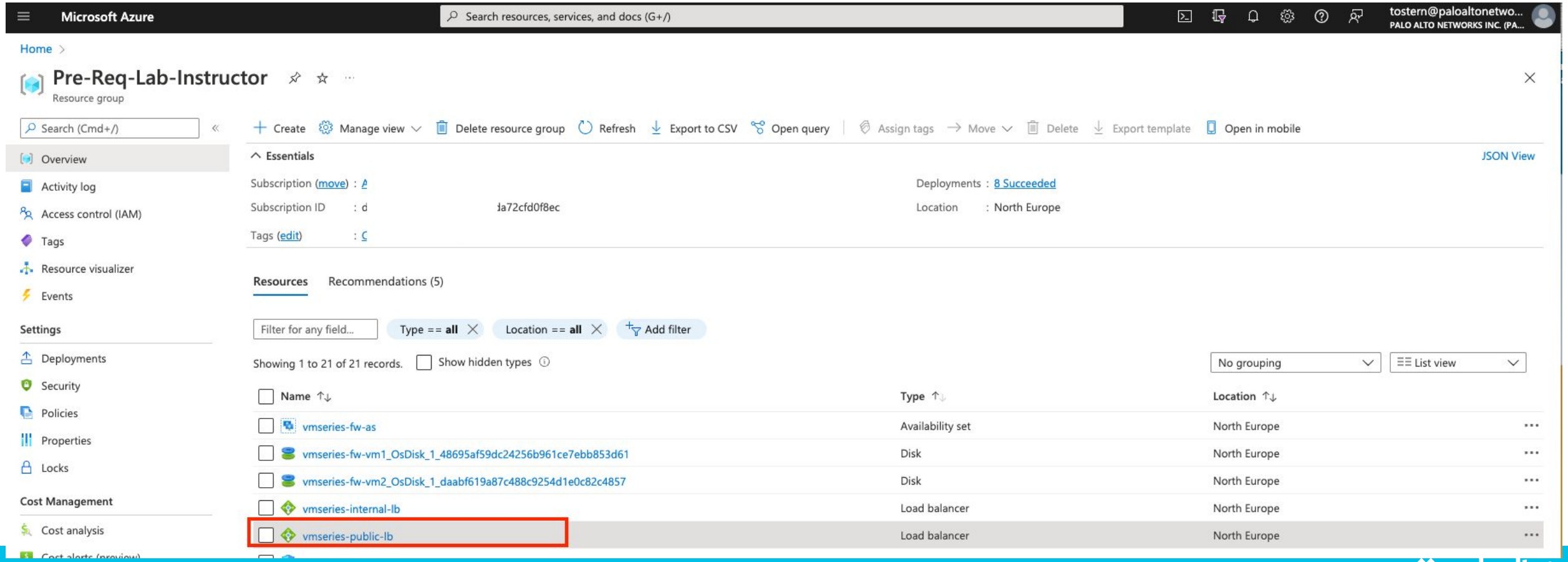
How to find Frontend IP addresses of Internal Load Balancer?

- In the Internal Load Balancer page select the **“Frontend IP configuration”**
- Copy the IP address of the **“LoadBalancerFrontEnd”**



How to find Frontend IP addresses of the Public Load Balancer?

- Navigate to your resource group you created here and select the **“vmseries-public-lb”**

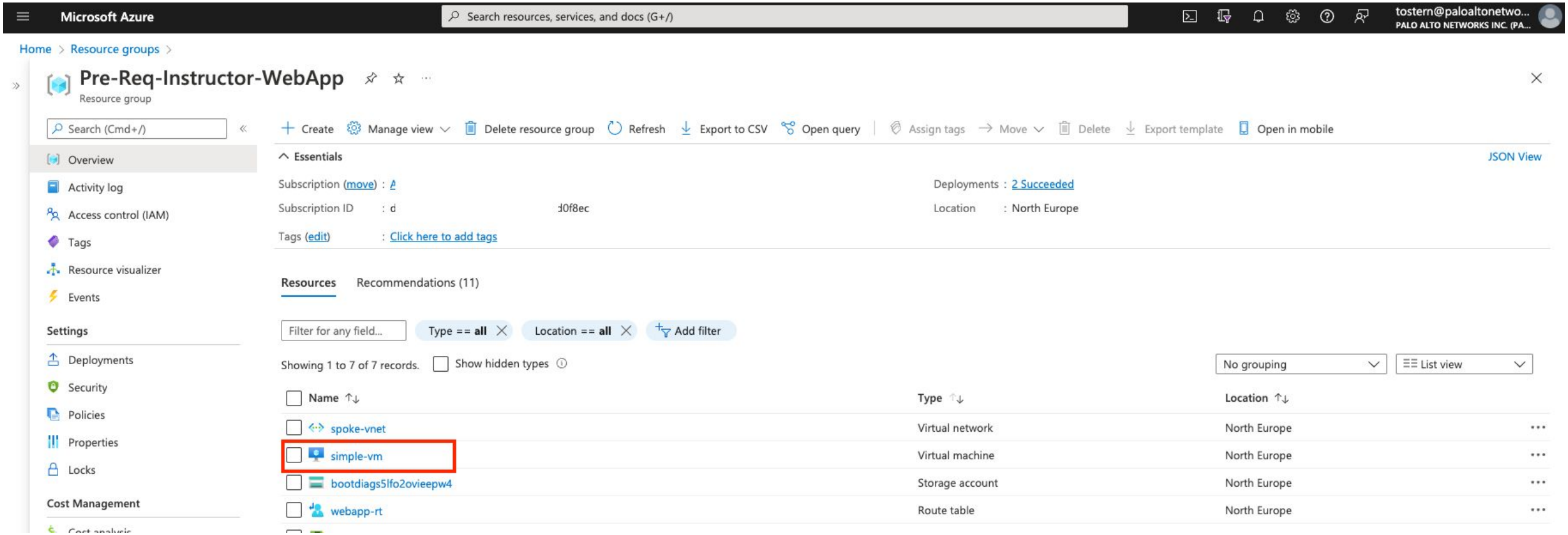


How to find Frontend IP addresses of Public Load Balancer?

- In the Internal Load Balancer page select the **“Frontend IP configuration”**
- Copy the IP address of the **“LoadBalancerFrontEnd”**

How to find the IP addresses of my Web Server?

- Navigate to your resource group you created here and select the **“simple-vm”**



How to find the IP addresses of my Web Server?

- Stay on the Virtual Machine overview page
- Copy the IP address of the **“Private IP address”**