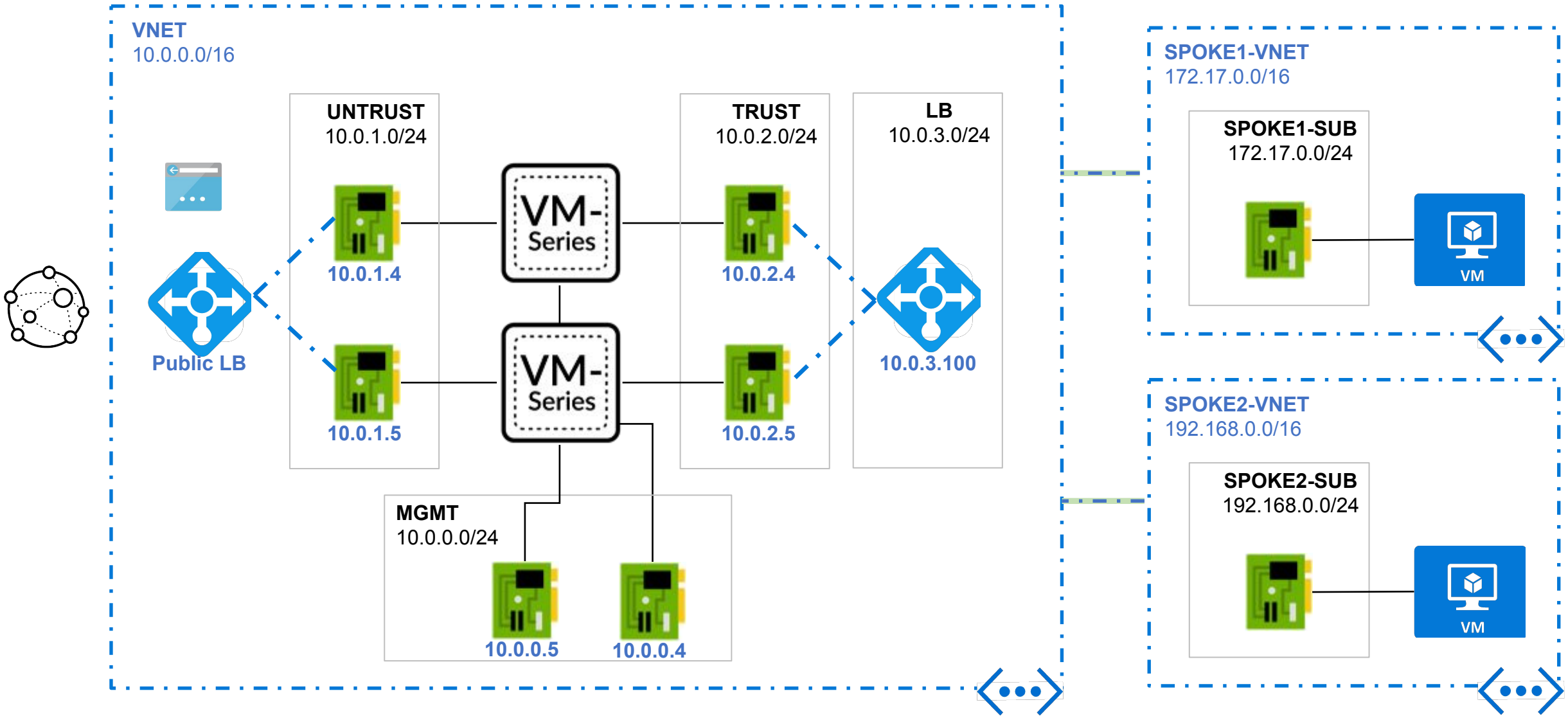
PRISMA
BY PALO ALTO NETWORKS

Prisma Public Cloud - Azure

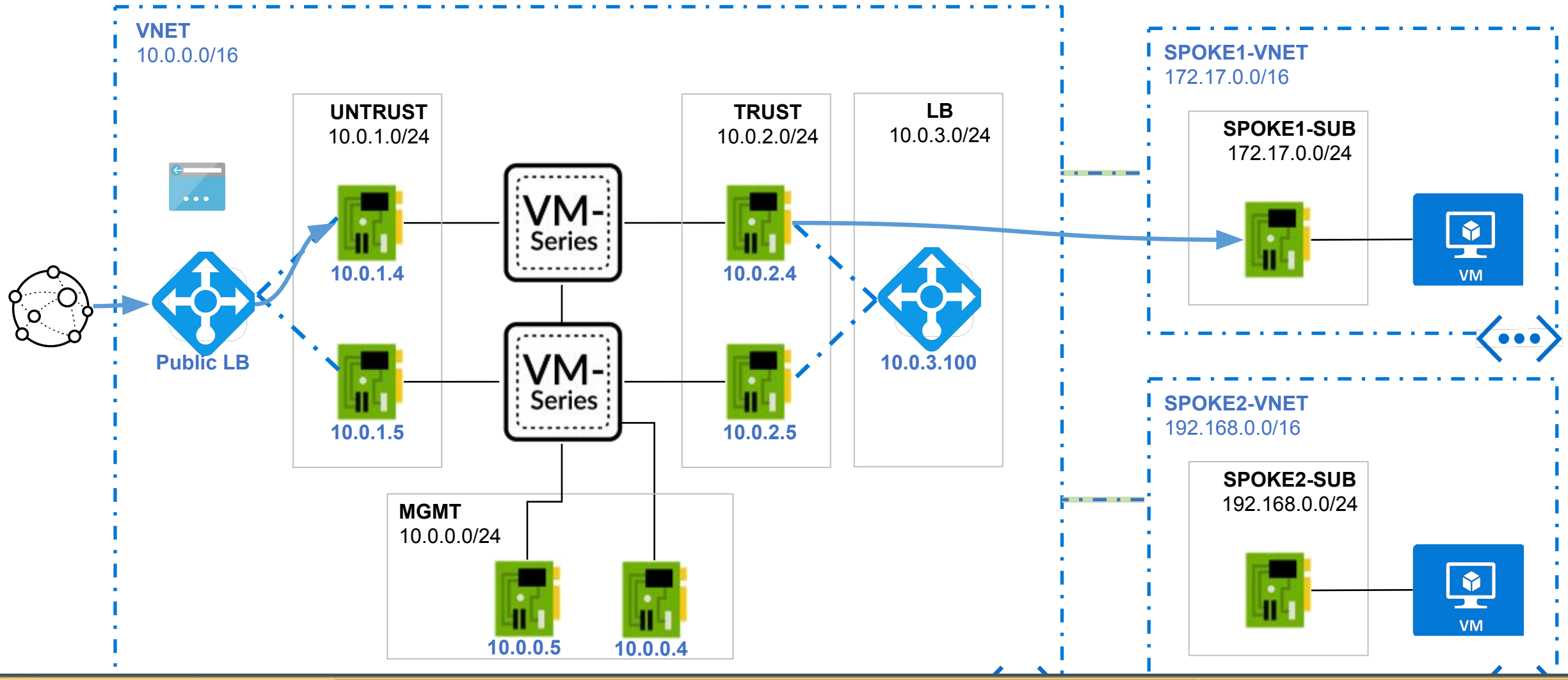
Lab Guide

paloalto NETWORKS

FOR THIS DESIGN, HOW DO I CONFIGURE THE VM-SERIES MANUALLY?

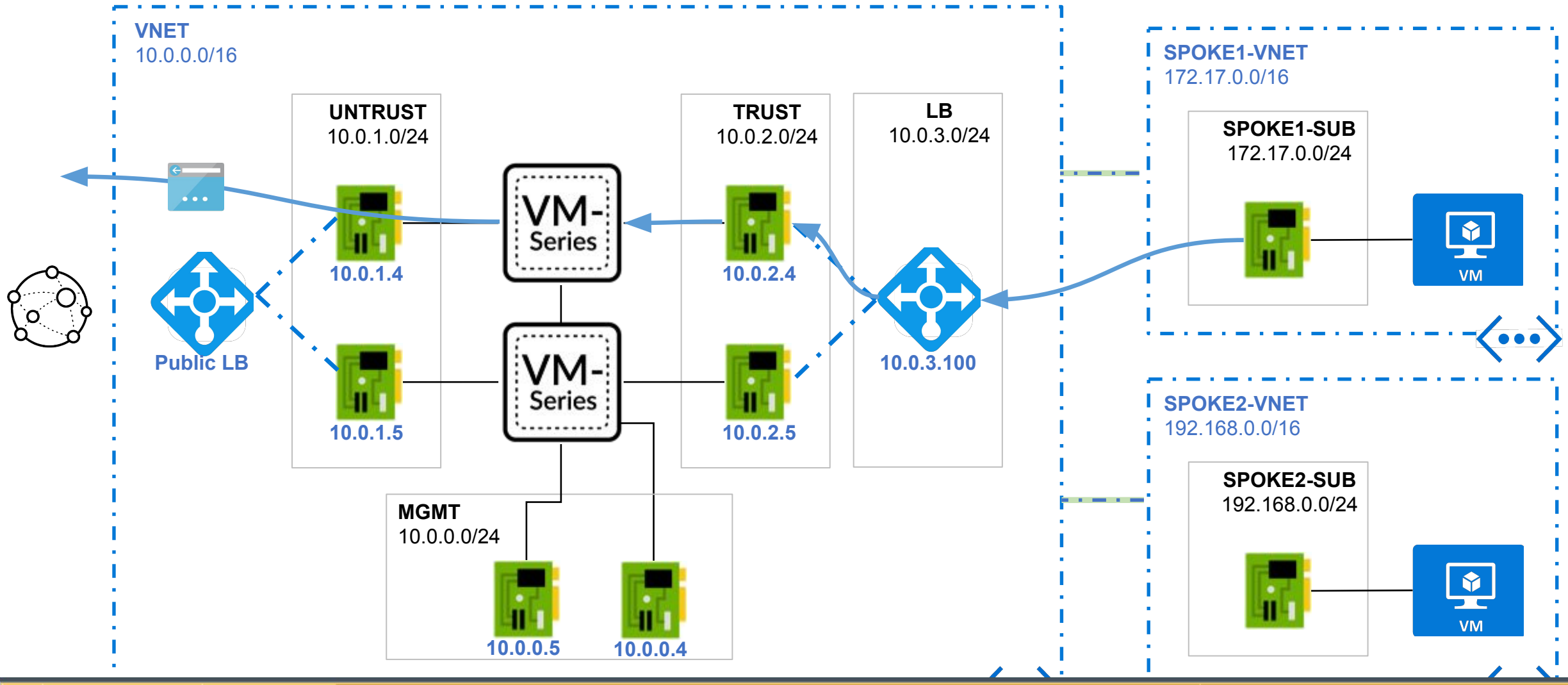


INBOUND TRAFFIC FLOW



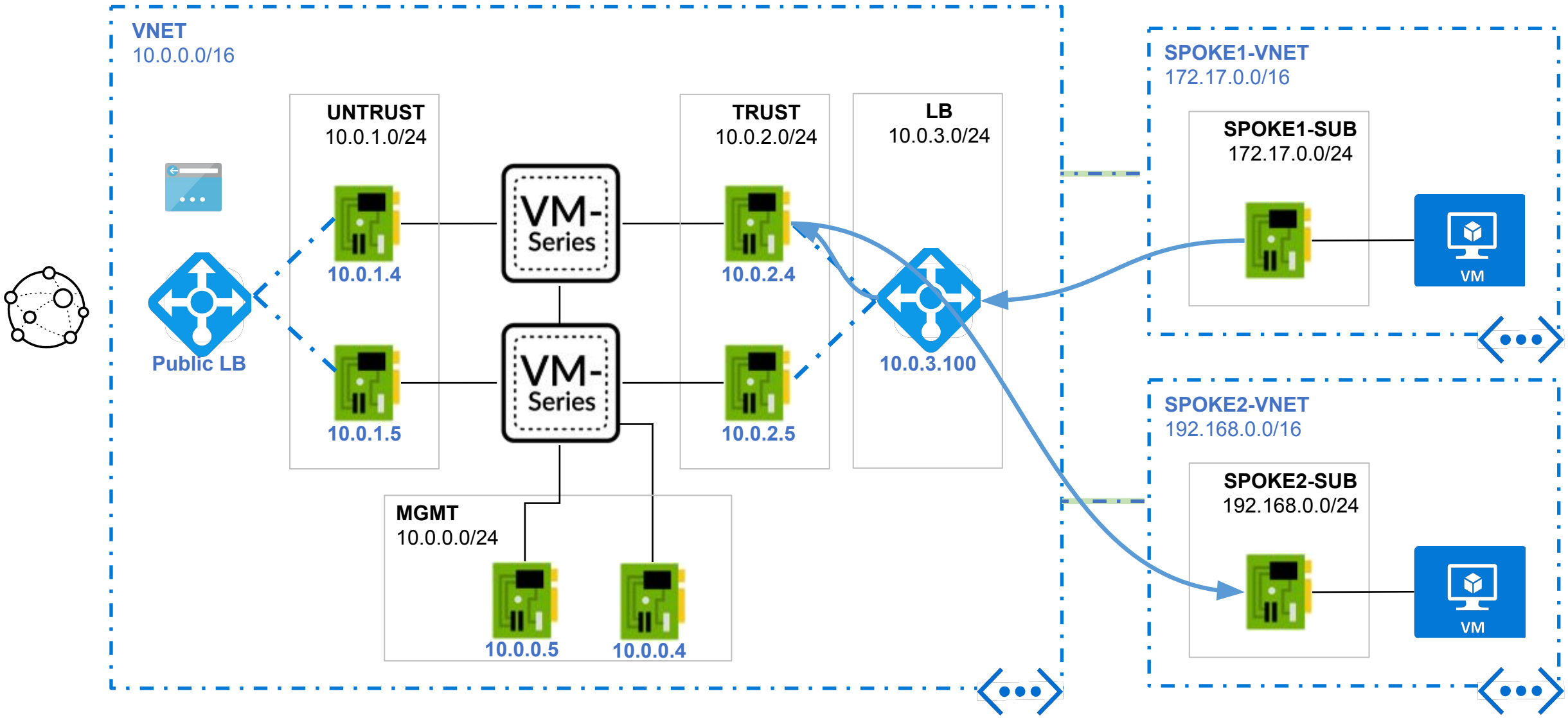
			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
2	inbound-spoke1	none	untrust-zon...	untrust-zone	any	any	untrust-nic	any	dynamic-ip-and-port ethernet1/2	destination-translation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

OUTBOUND TRAFFIC FLOW CONFIGURATION



			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 CONFIGURATION

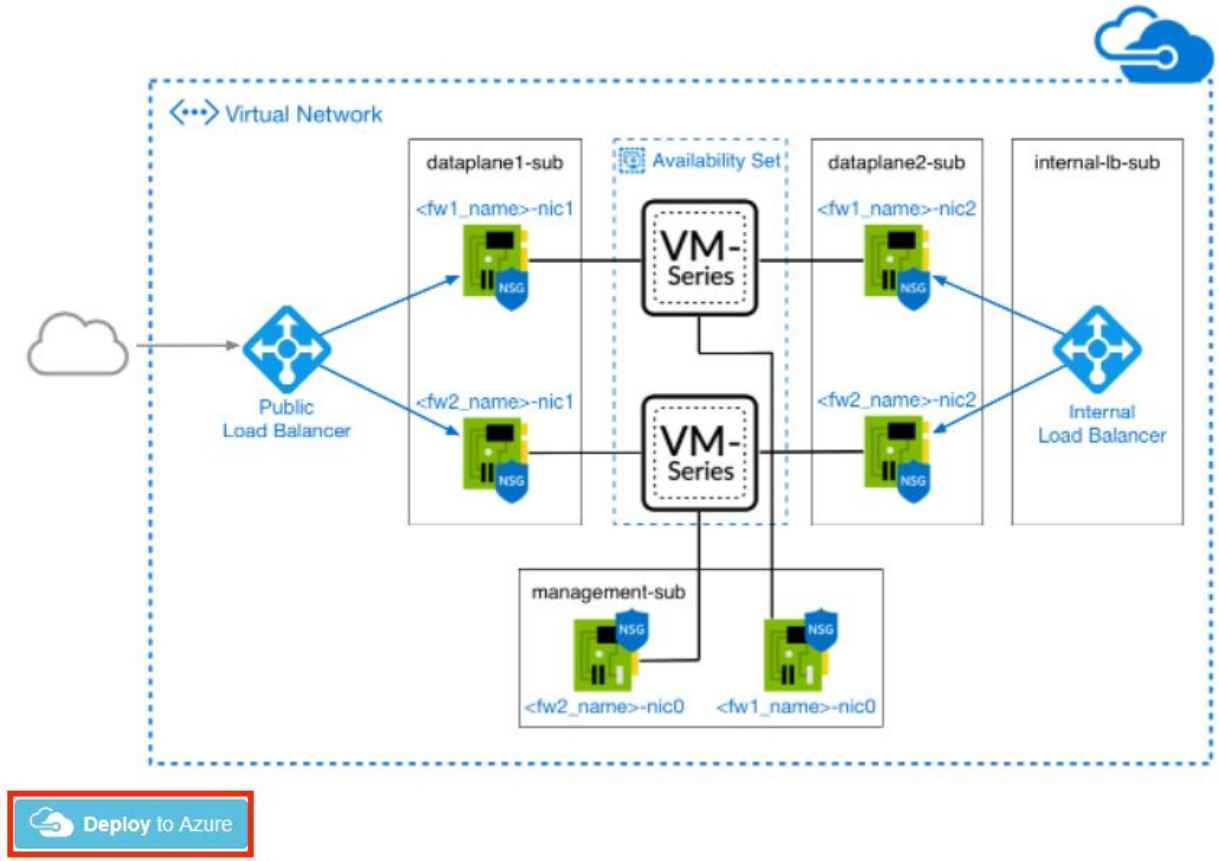


Deploy environment

Deploy Environment

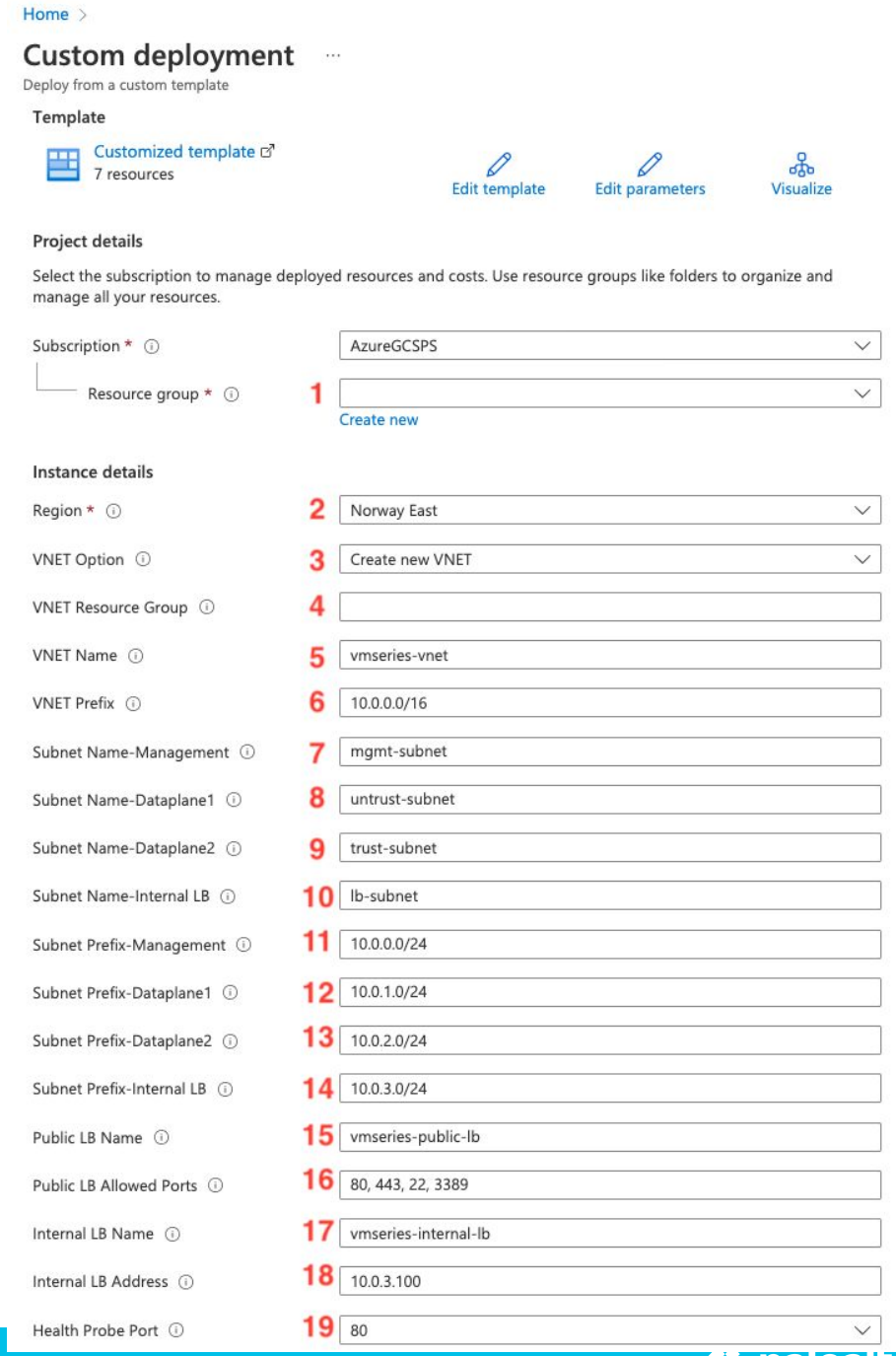
1. Click on the Link
   https://github.com/PaloAltoNetworks/lab-azure-vmseries

2. Click on “Deploy to Azure”



Deploy Environment

1. 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

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

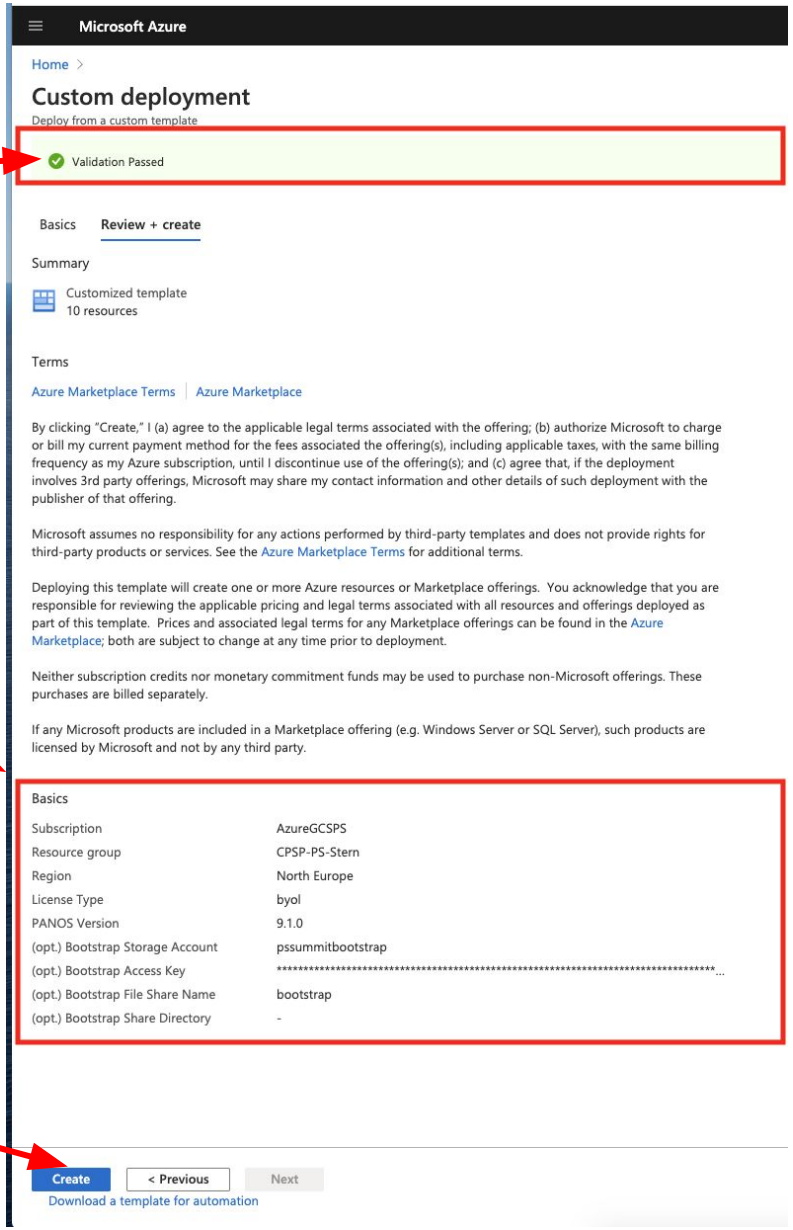
Check the box and click **“Next: Review + create”**

Deploy Environment

Check that the “Validation Passed”

Validate/Review the configuration

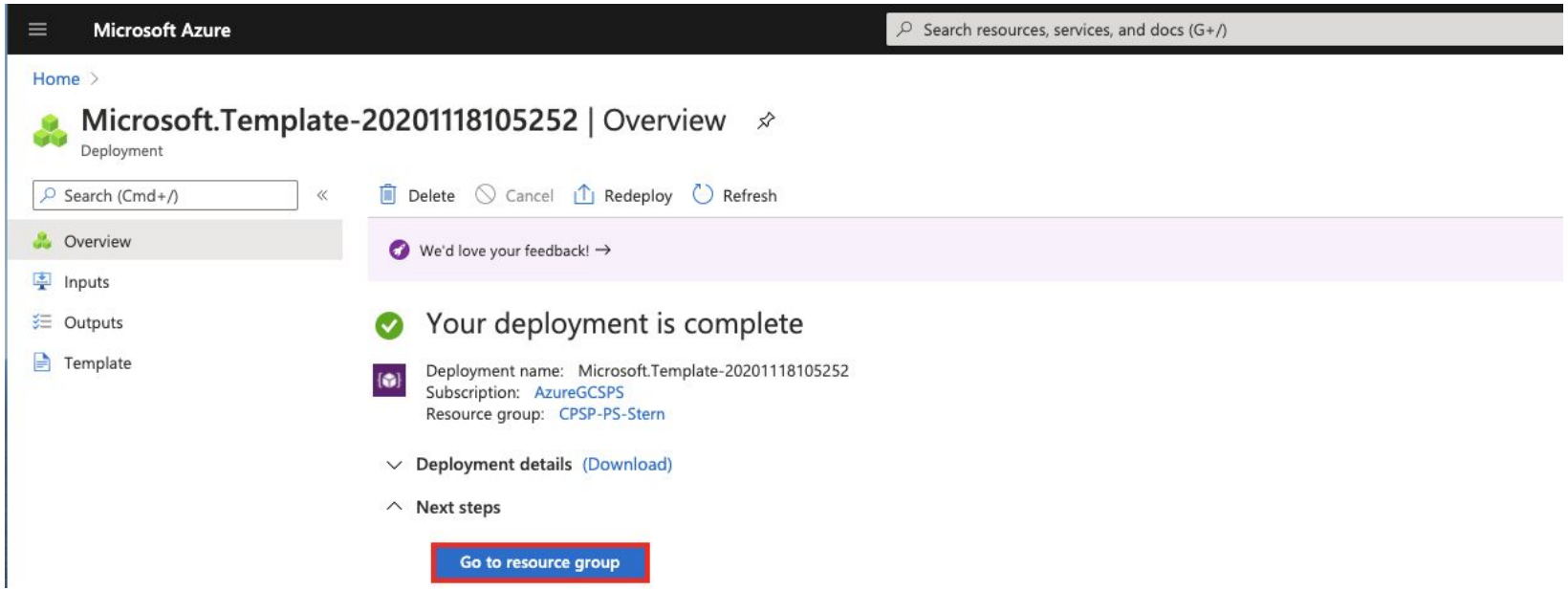
Click **“Create”**



Deploy Environment

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

Deployment can take up to 30 min! Coffee break!



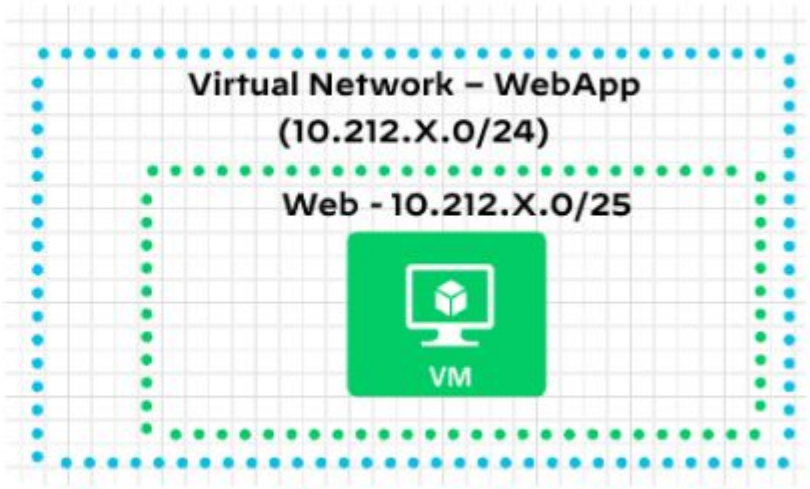
Deploy WebApp Resource Group

Deploy WebApp

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

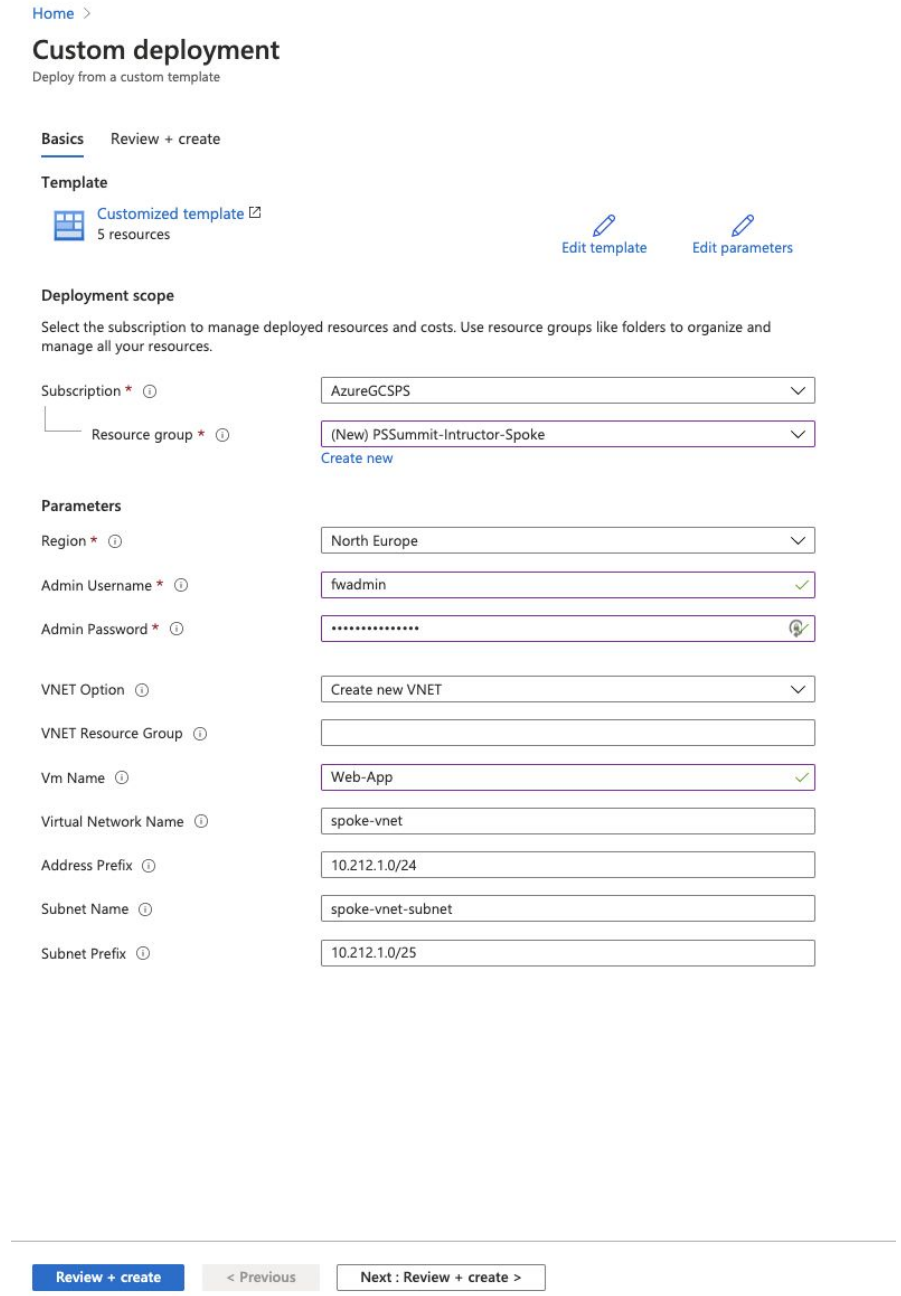
   https://github.com/PaloAltoNetworks/lab-azure-vmseries

2. Click on “Deploy to Azure”



Deploy WebApp Spoke

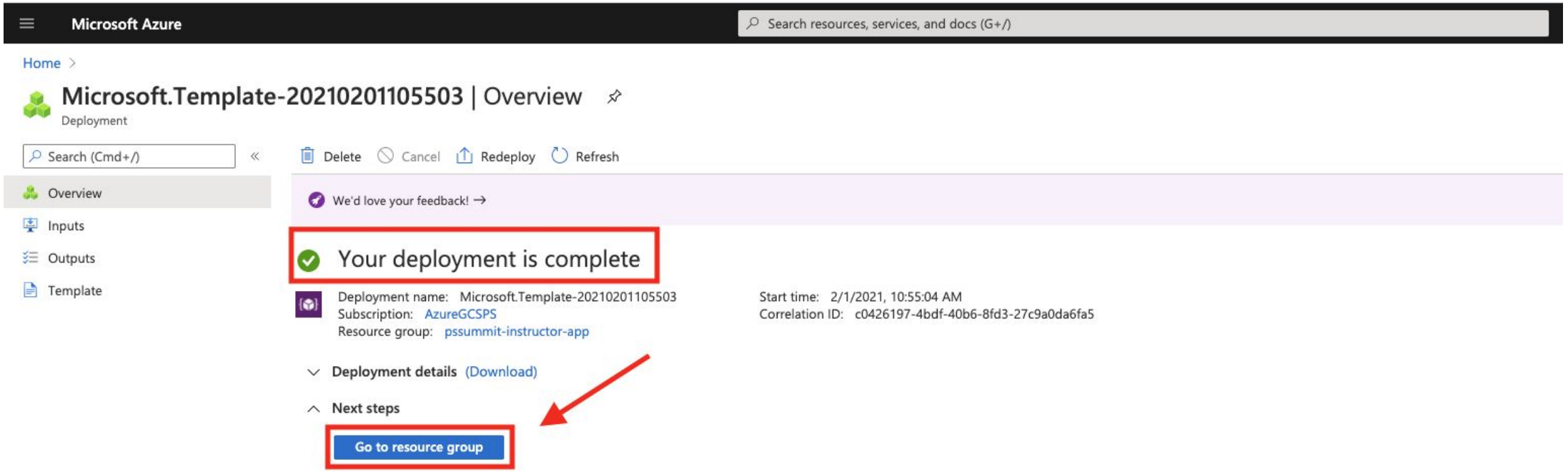
1. Create a new Resource Group (Azure-Lab-Spoke1<NAME>
2. Select any Region
3. Your prefered Username
4. Your prefered Password
5. Select “Create new VNET”
6. Empty
7. Web-App-<Name>
8. VNET-Spoke-<Name>
9. Don’t Change
10. Don’t Change
11. VNET-Spoke-subnet<Name>
12. Don’t Change



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

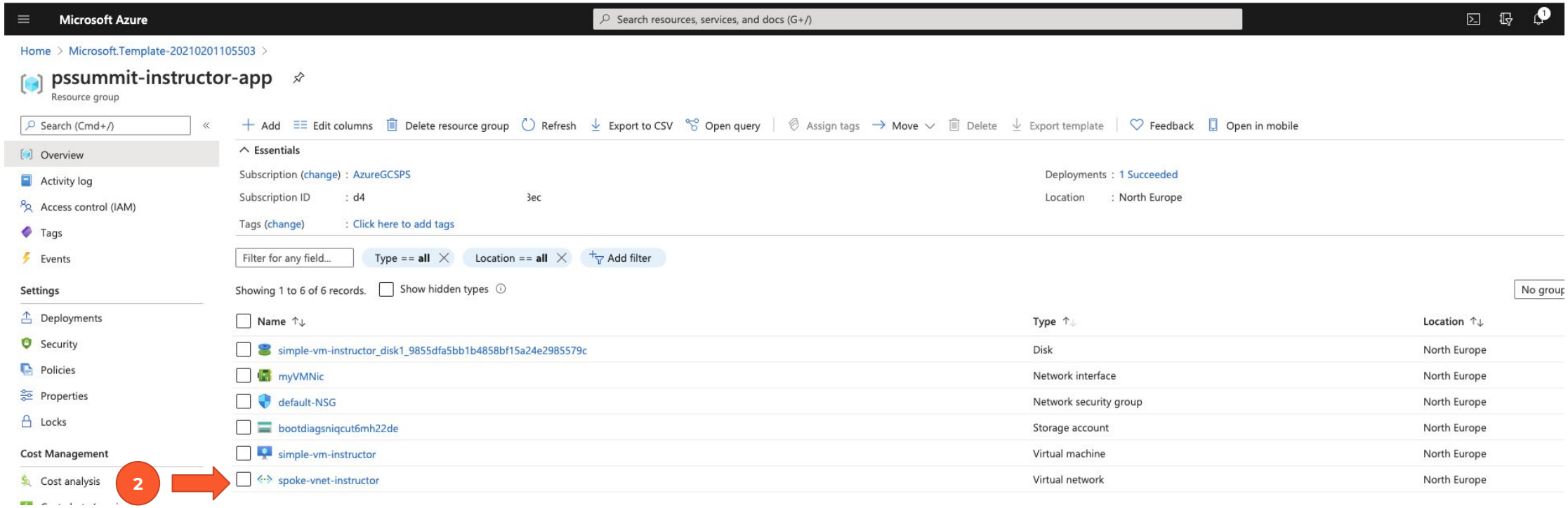
1. **Create Virtual Network Peerings** between the newly deployed “Hub” and any applications Virtual Networks.
2. **Create Security Policy** in Panorama to allow traffic to flow.
3. **Create a Route Table** in the Application Virtual Networks to forward traffic to the “Egress Private IP” which is the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

Deploy WebApp Resource Group

Create VNet Peering

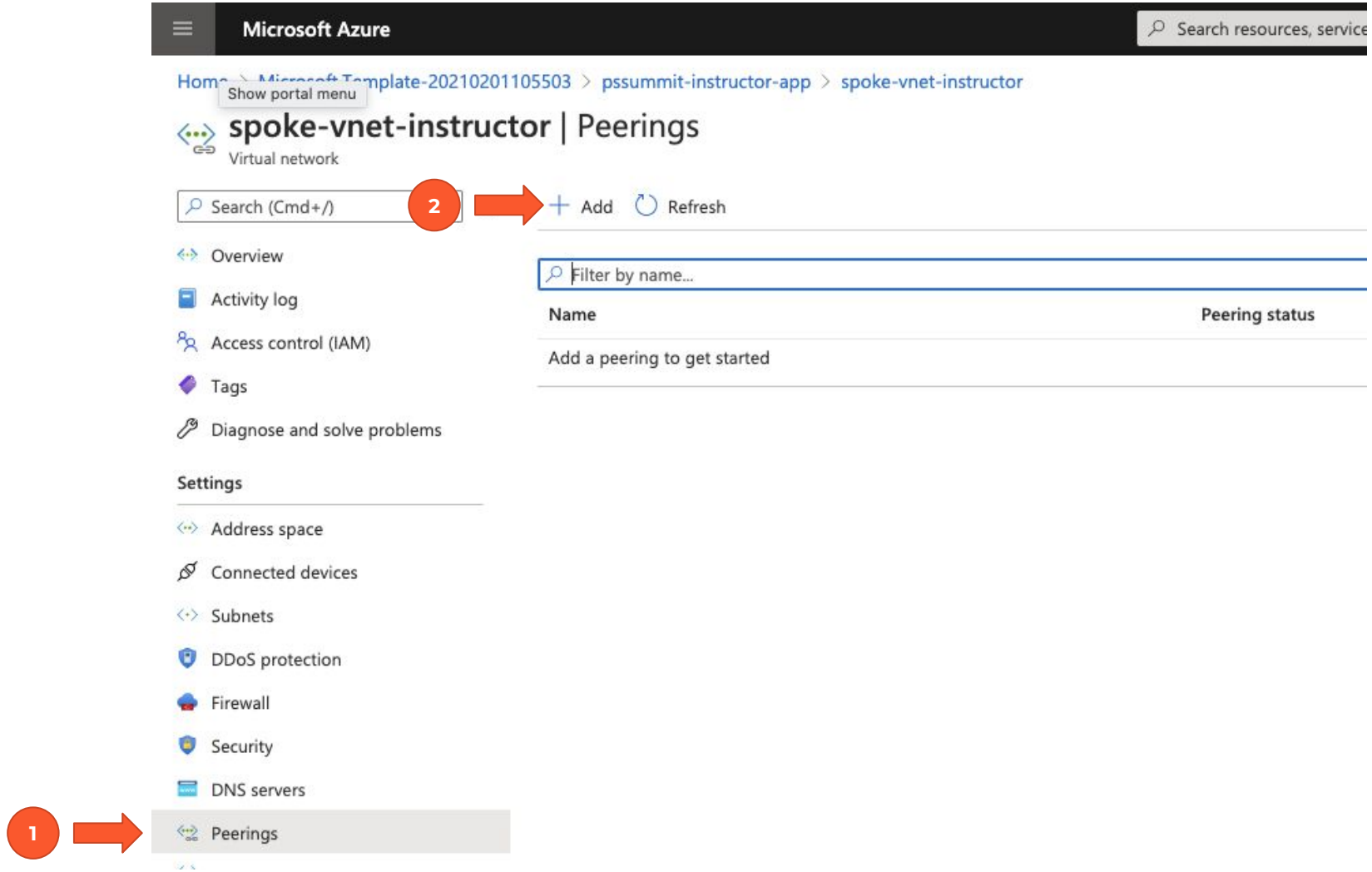
Create VNET peering

- Select the Virtual Network



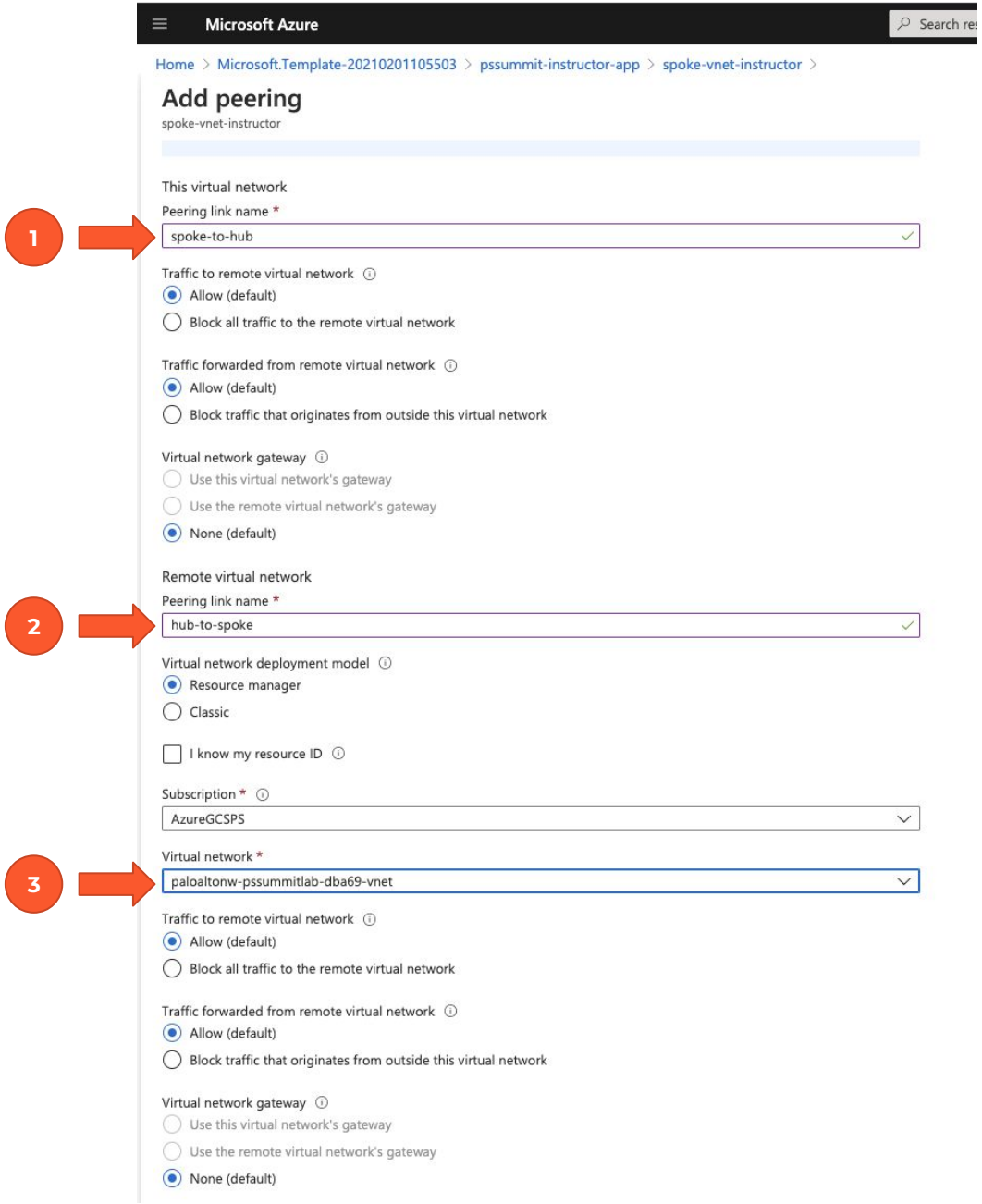
Create VNET peering

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



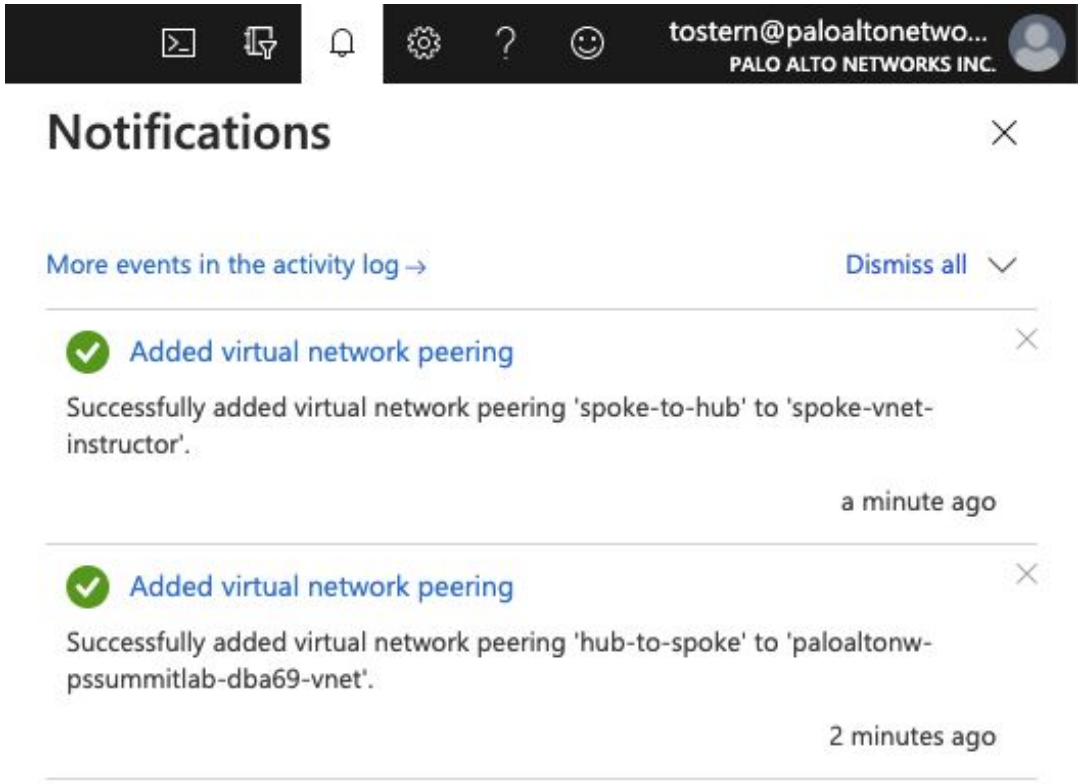
Create VNET peering

1. Use the same name
2. Use the same name
3. Select here the VNET of the created Deployment
4. Select Create



Validate VNET peering

When the peering was successful you should see the following the Azure logs

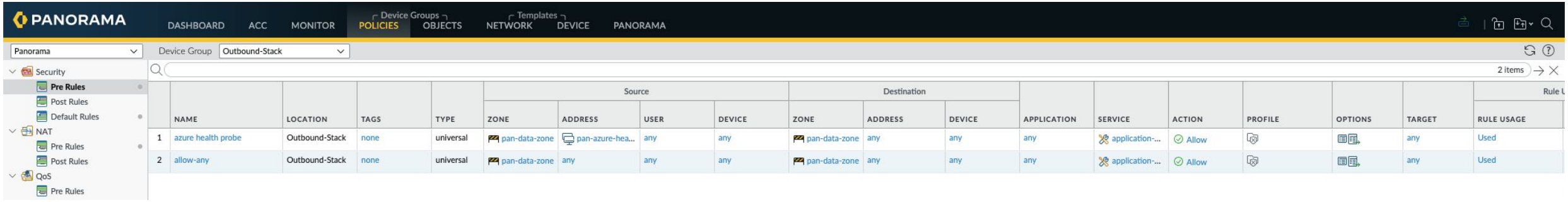


Deploy WebApp Resource Group

Create Outbound Security Rule

Create Security Policy

- Create an “Any-Allow” rule under the Outbound Stack
- This guarantee that we didn’t run into any issues during the testing. See Example below

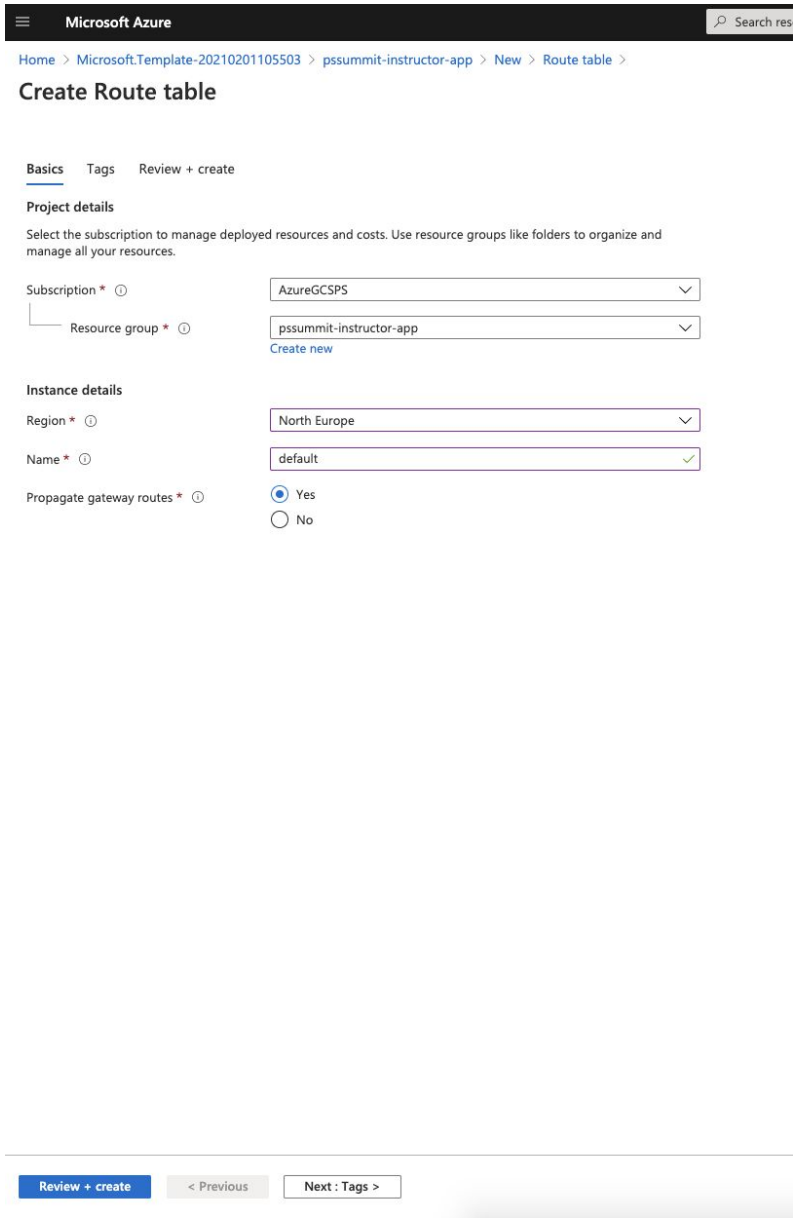


Deploy WebApp Resource Group

Create/Configure Route Table

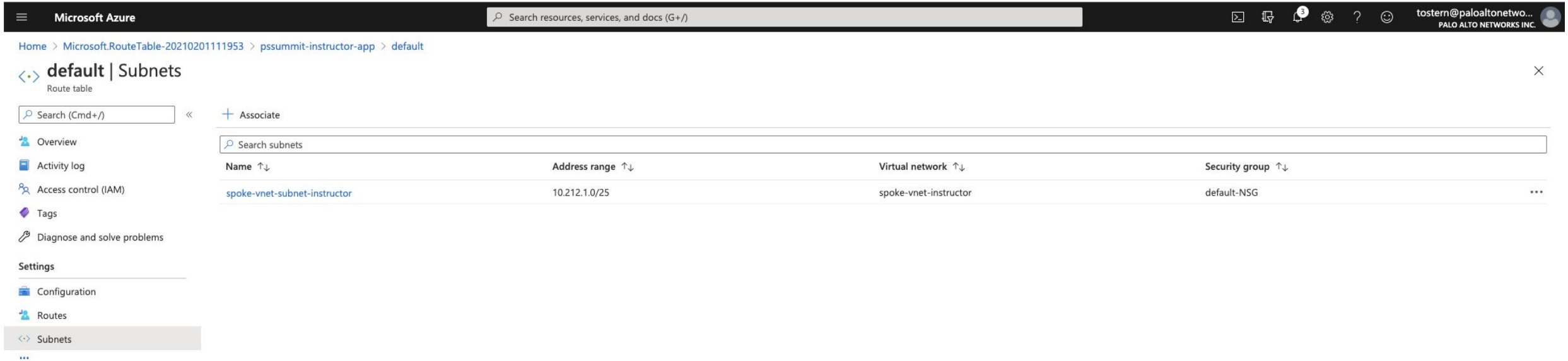
Create Web-App Route table

1. Create a Route table into your Application Resource Group
2. Use the values as in the example
3. Click “Review+Create
4. When the Validation is successful click on “Create” in the next window



Associate Route table with subnet

1. Select the previous create route table
2. Click on Subnets → Associate and select the Subnet of your Application subnet



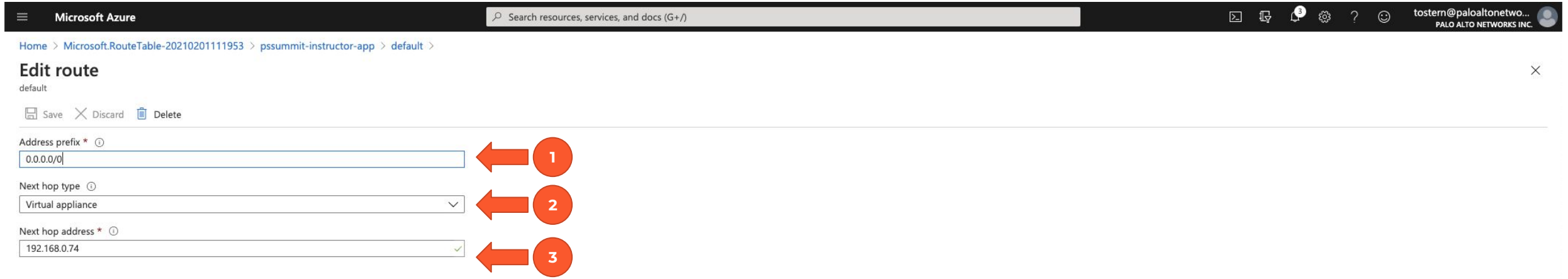
Create static Route

1. Select Routes
2. Click Add

Create static Route

1. Address prefix: 0.0.0.0/0
2. Next hop type: Virtual Appliance
3. Next hop address: Private Frontend IP of the Hub Internal Load Balancer
4. Select Save

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



Deploy WebApp Resource Group

Configure Web Server

Install / Update Web Web Server

1. Login into the Web Server via the Serial Console connection in Azure
   a. Activate Boot diagnostics when it isn't configured

2. Upgrade Web Server by using the following command
   a. sudo apt-get upgrade

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

Configure VM-Series

Configure Web Server

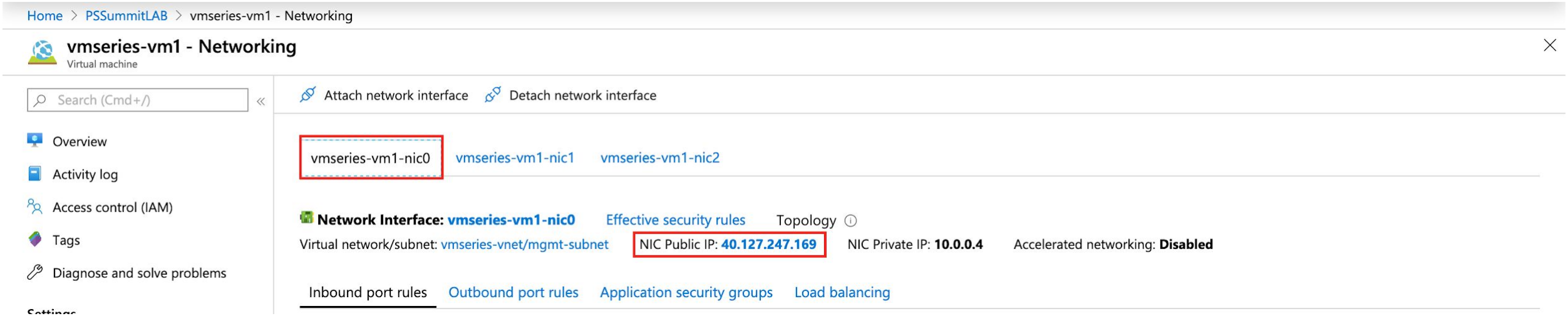
paloalto NETWORKS

Configure VM-Series

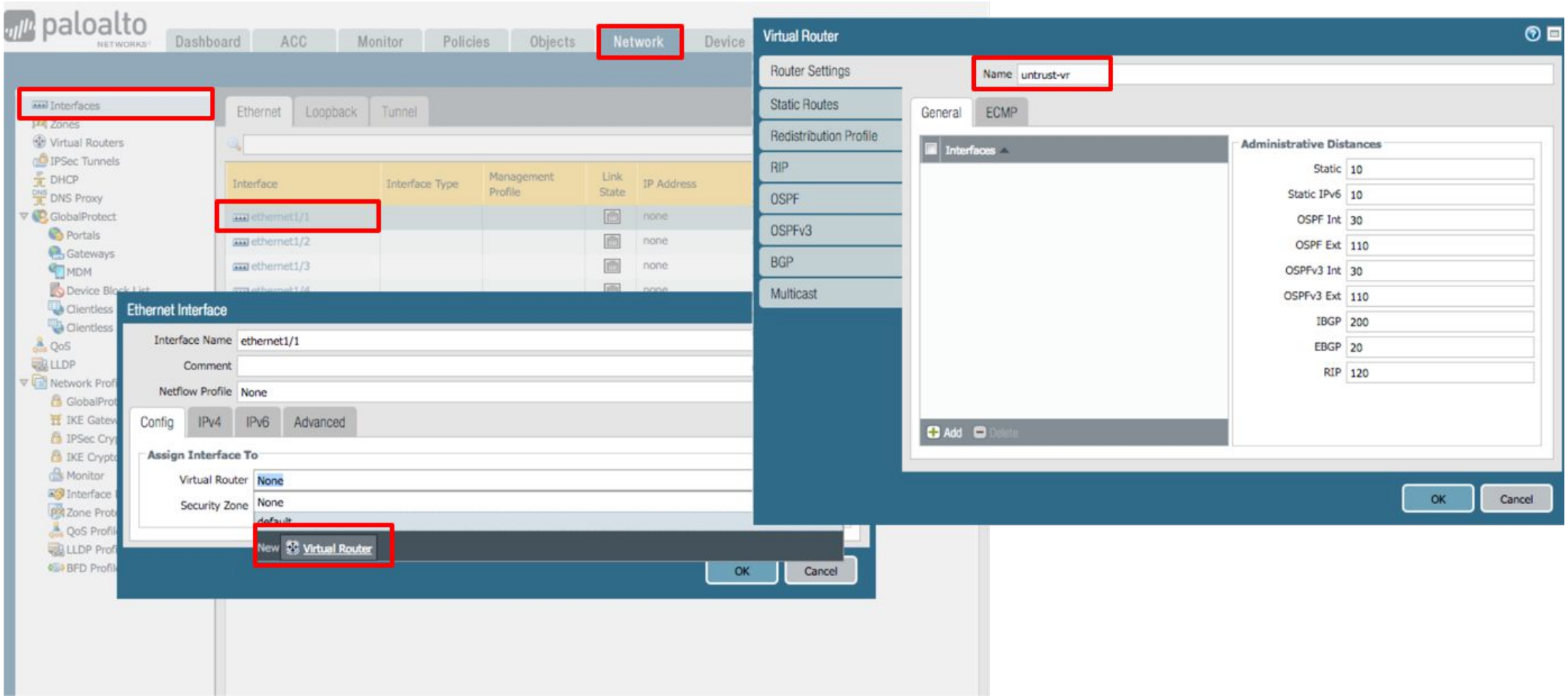
Interface Configuration

Log into FW1

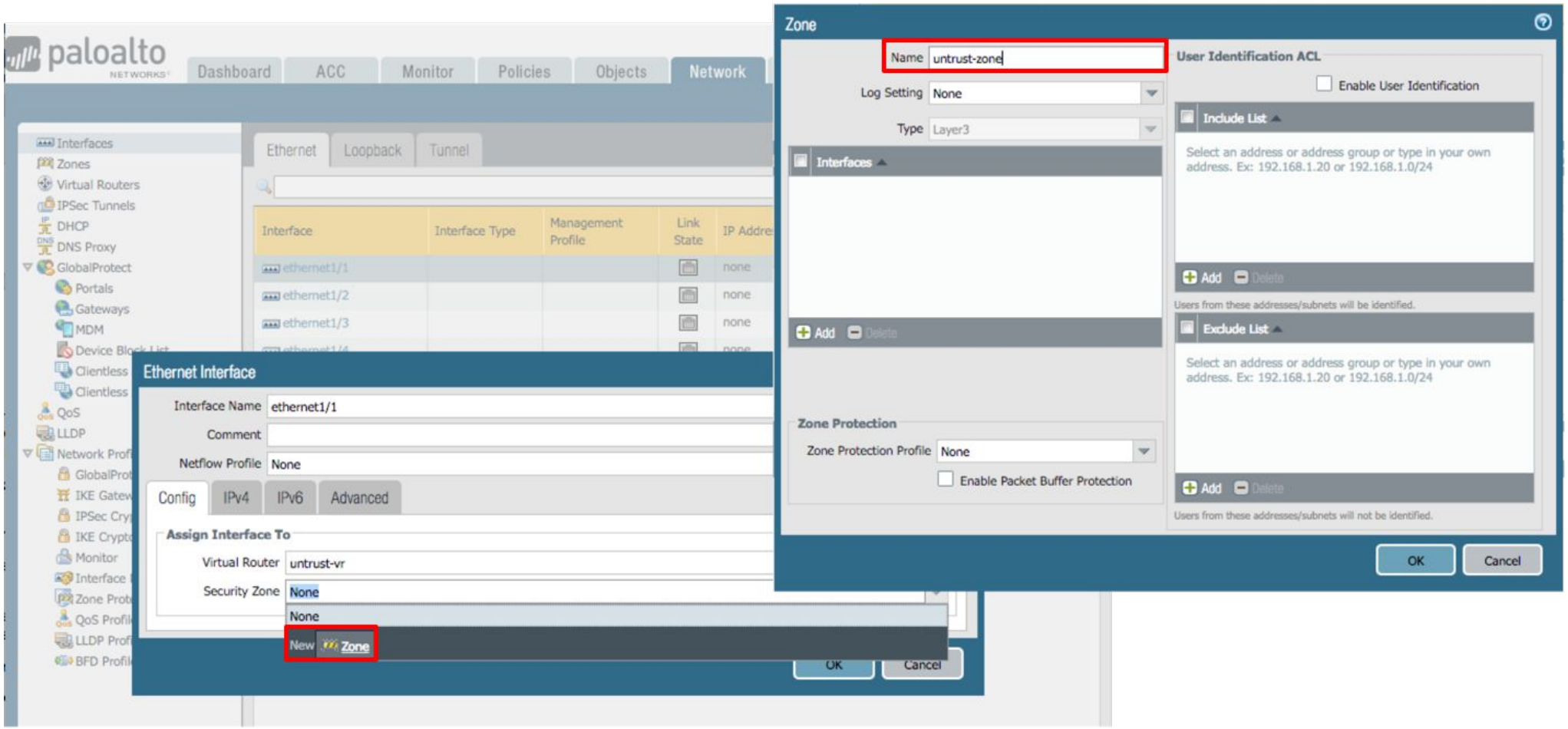
- Firewall and Backend VM credentials
- https://<vmseries_public_ip_on_first_interface>
- Username: paloalto
- Password: PanPassword123!



Configure Untrust Interface - Virtual Router

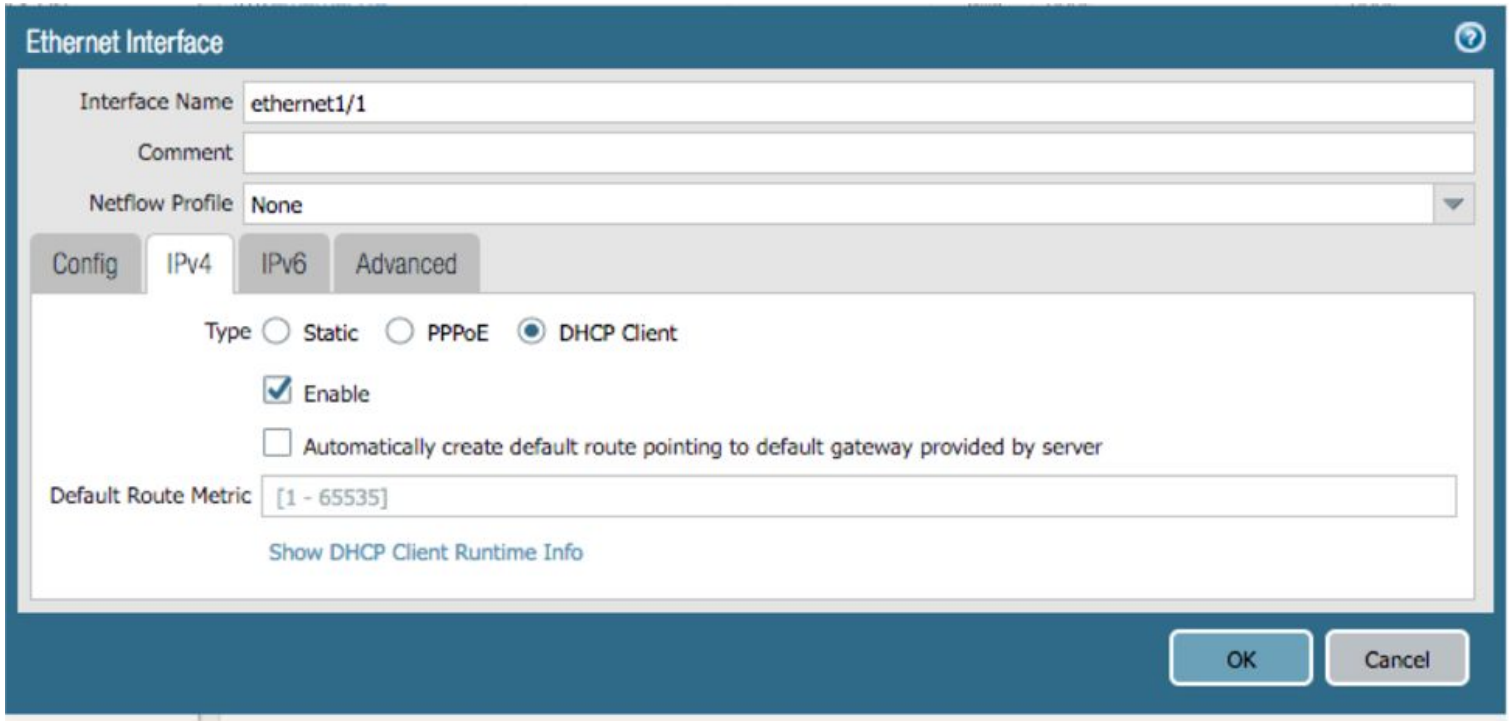


Configure Untrust Interface - Zone



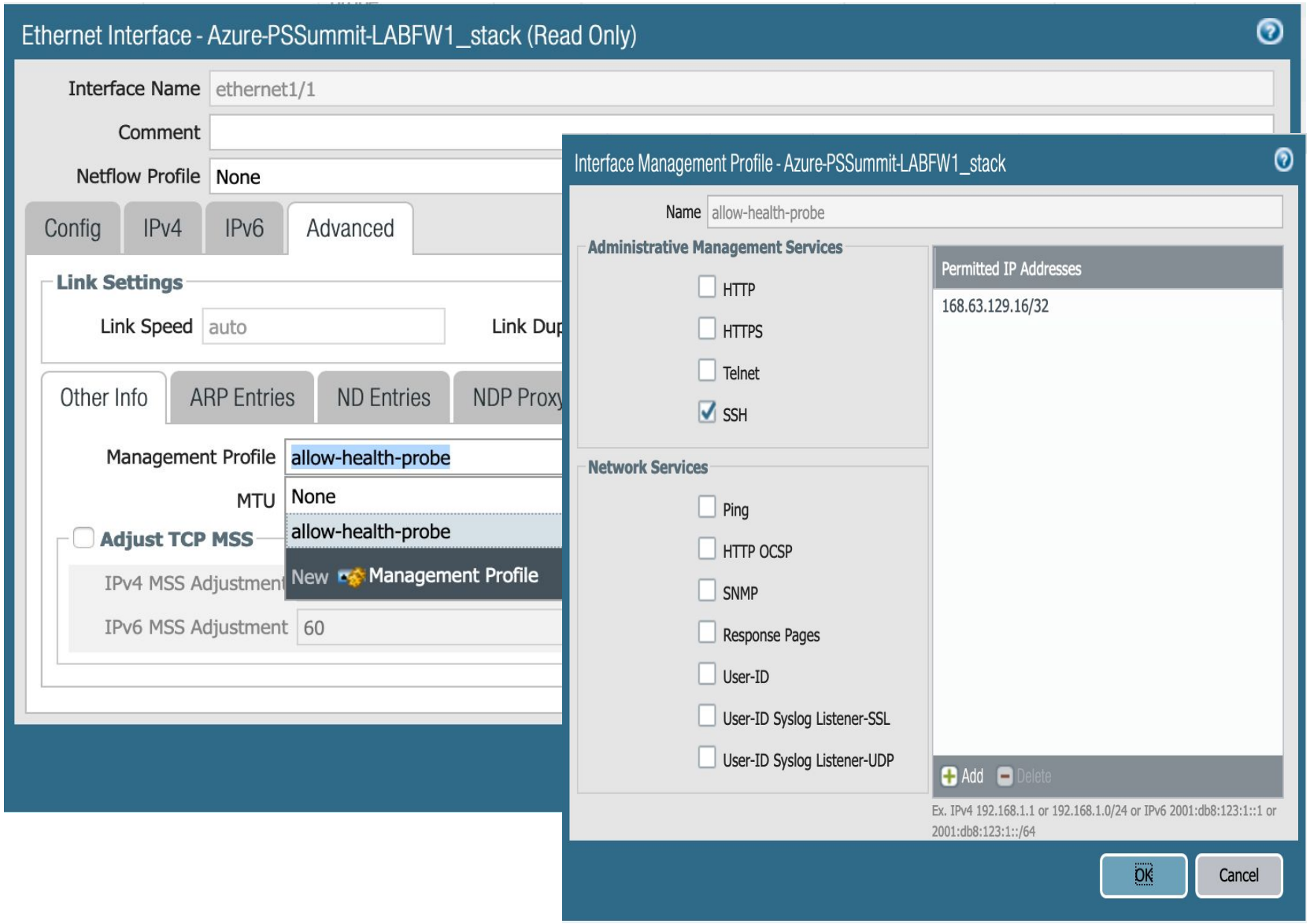
Configure Untrust Interface - DHCP

1. While still in side eth1/1, click IPv4 Tab
2. Check DHCP Client
3. Uncheck “Automatically create route pointing to default gateway server”

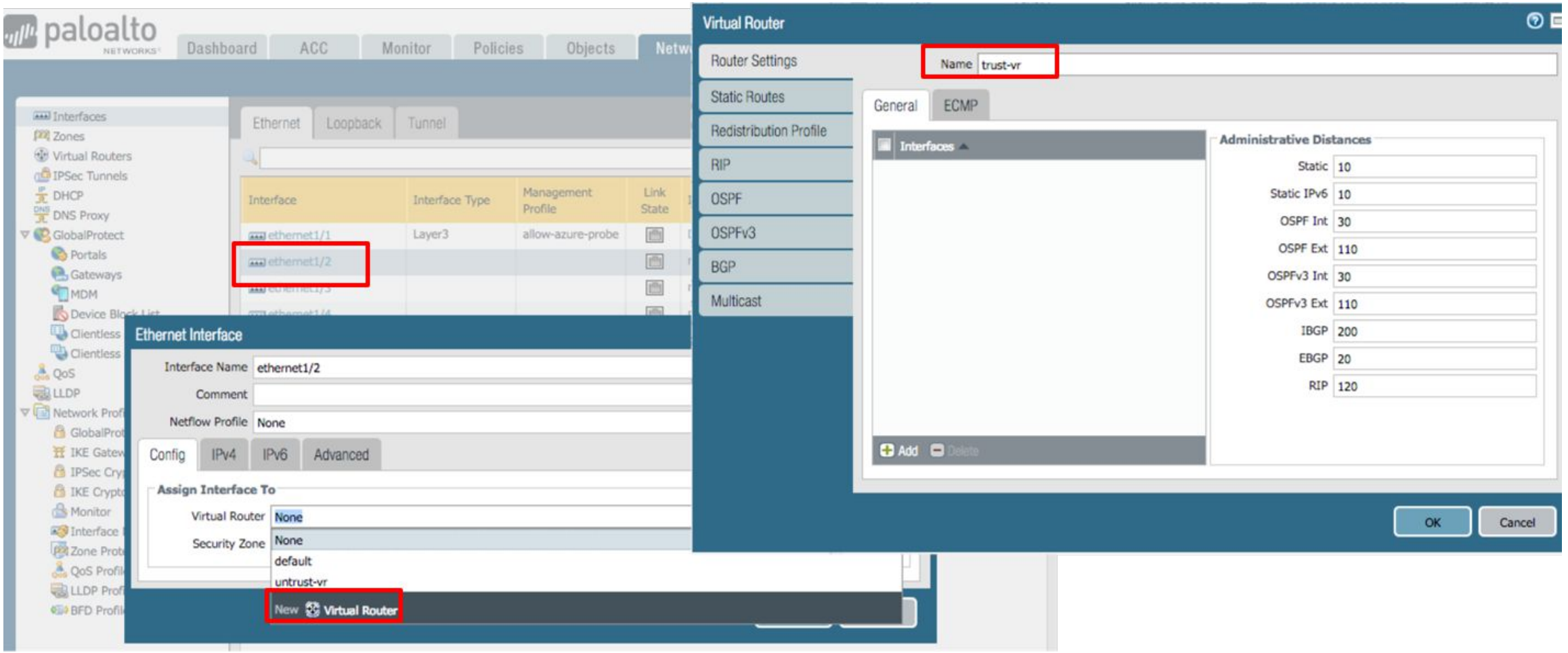


Configure Untrust Interface - Advanced

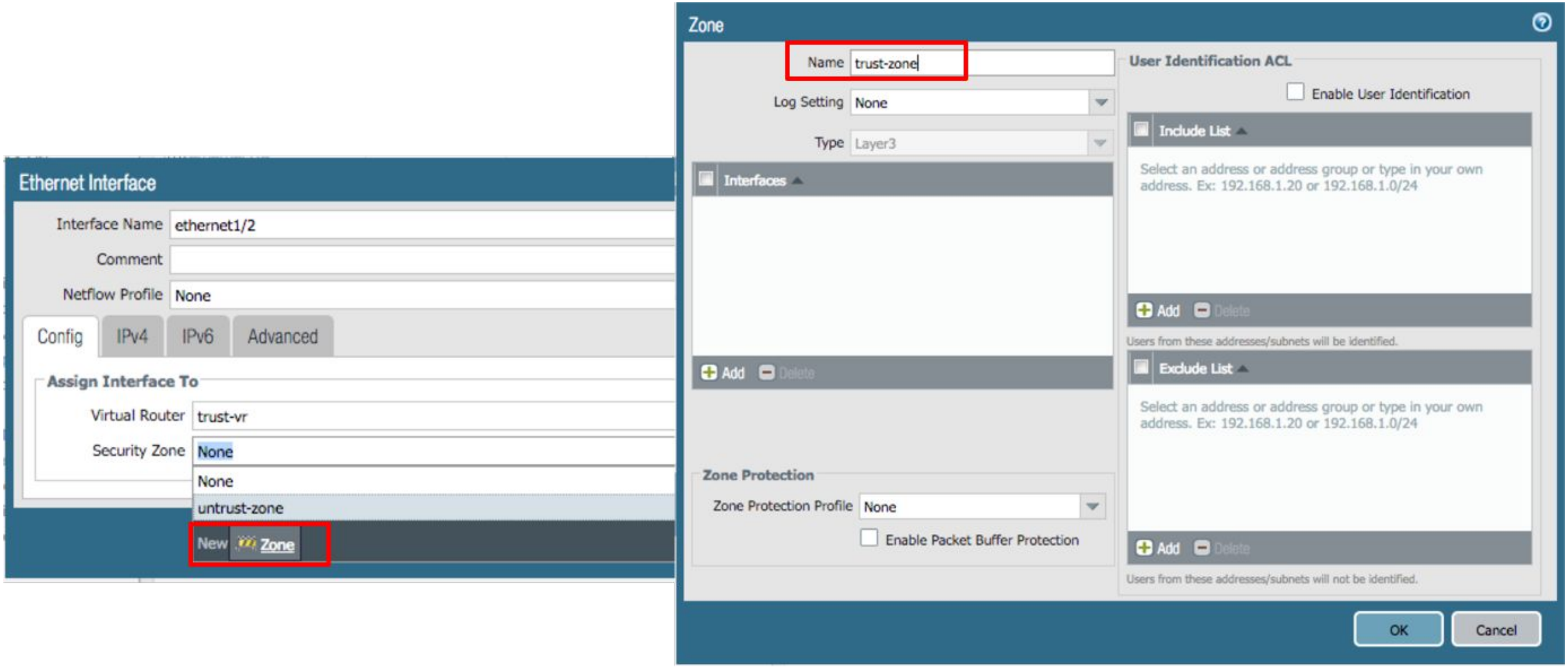
1. While still in side eth1/1, click Advanced Tab
2. Click the Management Profile dropdown and select “New Management Profile”
3. Check SSH
4. Permitted IP: 168.63.129.16/32
5. Click OK



Configure Trust Interface - Virtual Router

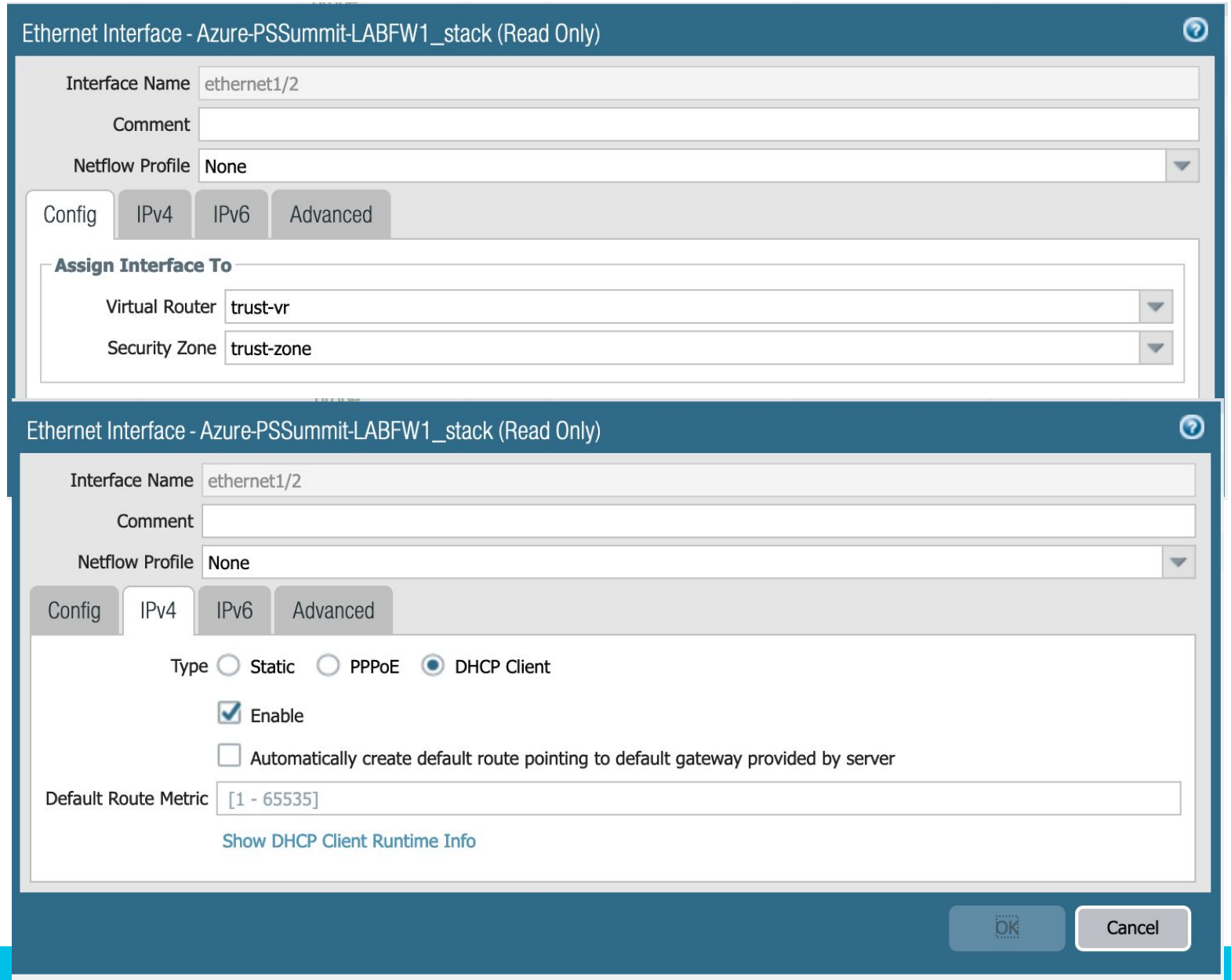


Configure Trust Interface - Zone



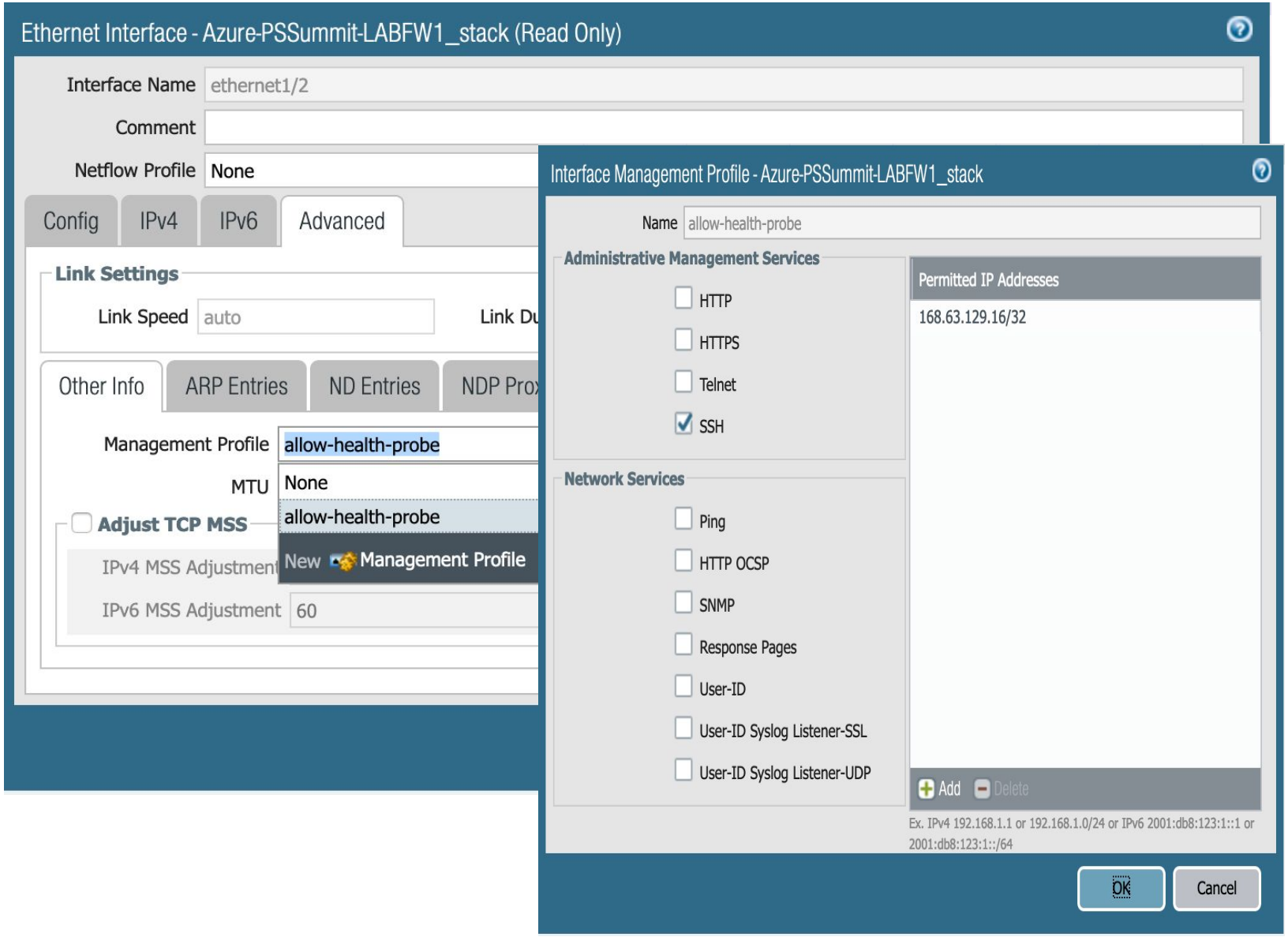
Configure Trust Interface - DHCP

1. While still in side eth1/2, click IPv4 Tab
2. Check DHCP Client
3. Uncheck “Automatically create route pointing to default gateway server”



Configure Trust Interface - Advanced

1. While still in side eth1/1, click Advanced Tab
2. Click the Management Profile dropdown and select the previous created profile



Repeat these steps on FW2 using the same settings

Configure VM-Series

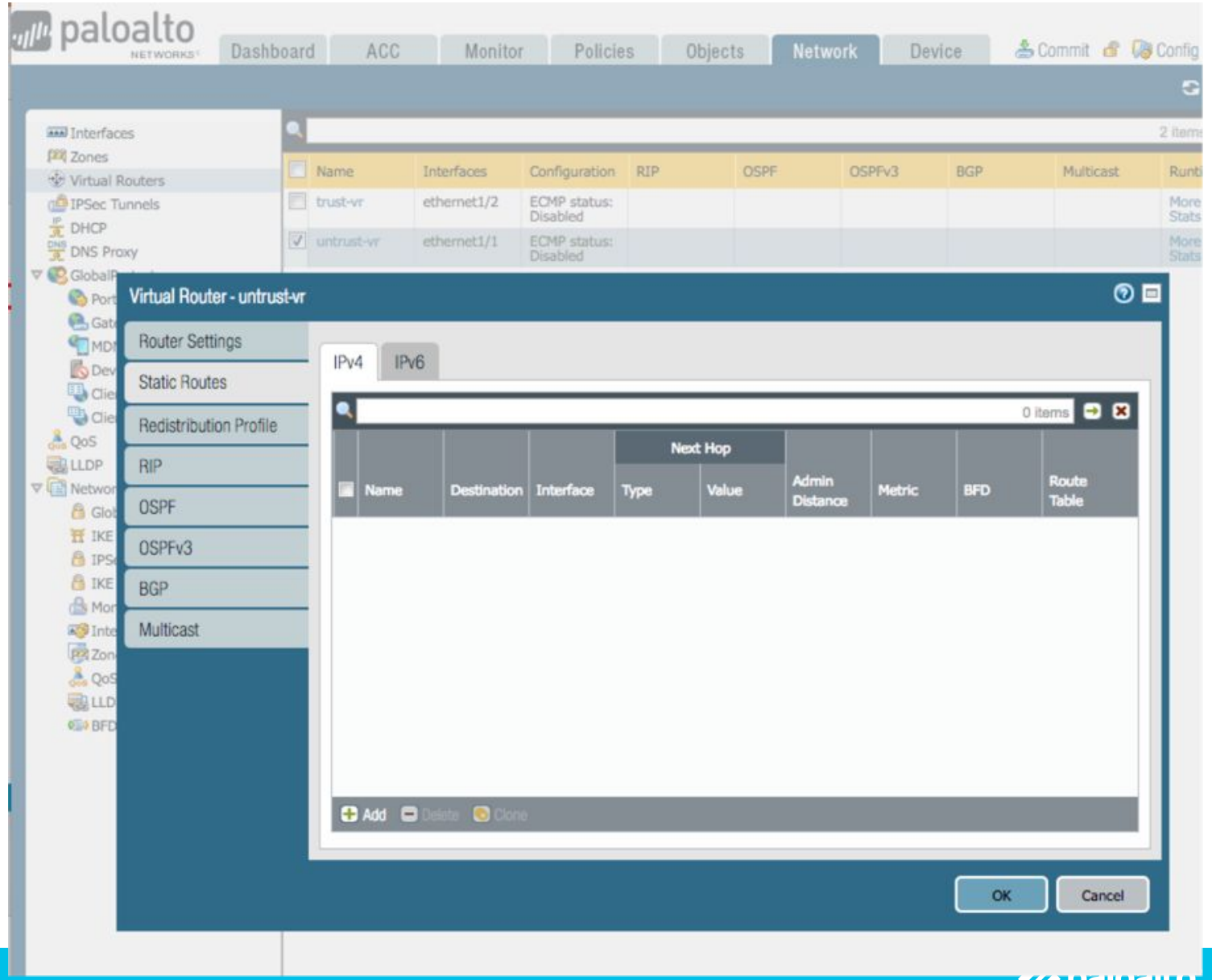
Routing on Virtual Routers

Configure Untrust VR

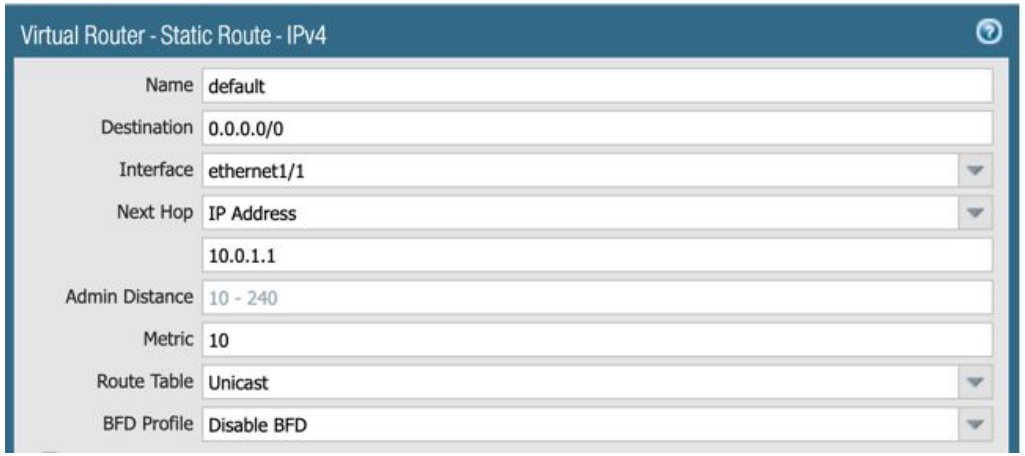
Go to:

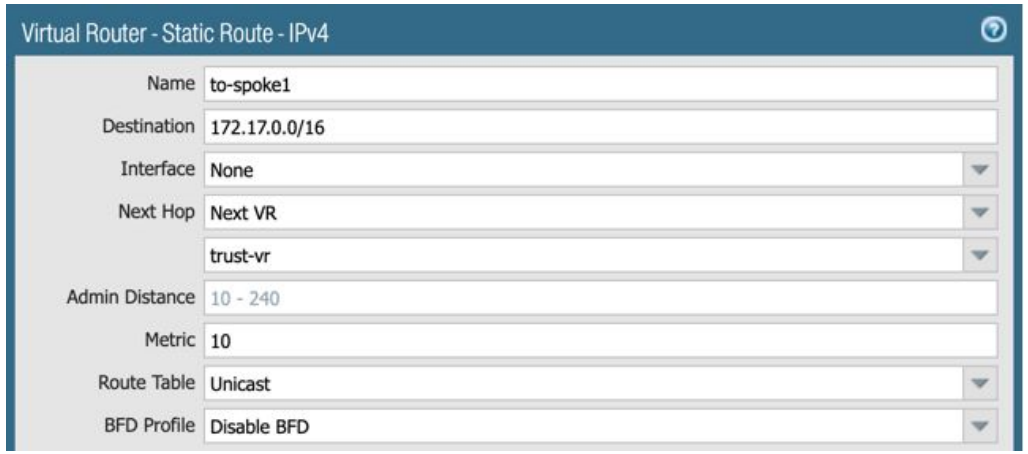
Network ⟶ Virtual Routers ⟶

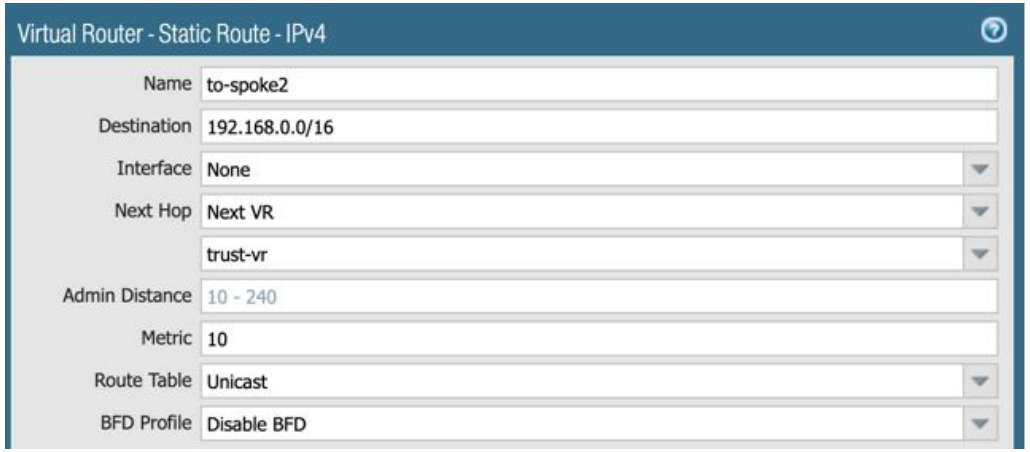
untrust-vr ⟶ Static Routes ⟶ Add



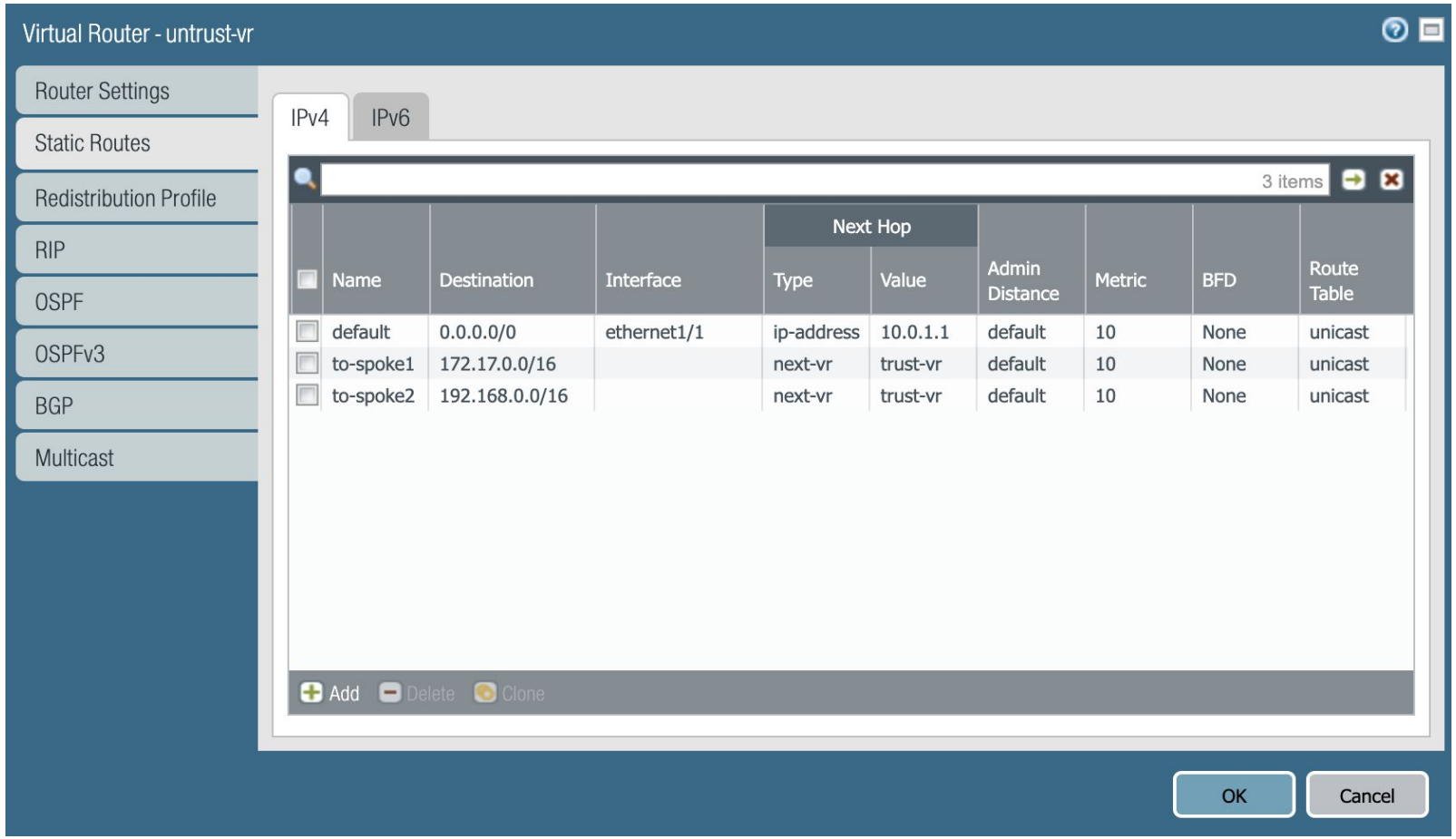
Configure Untrust VR - Static Routes







Configure Untrust VR - Static Routes Summary

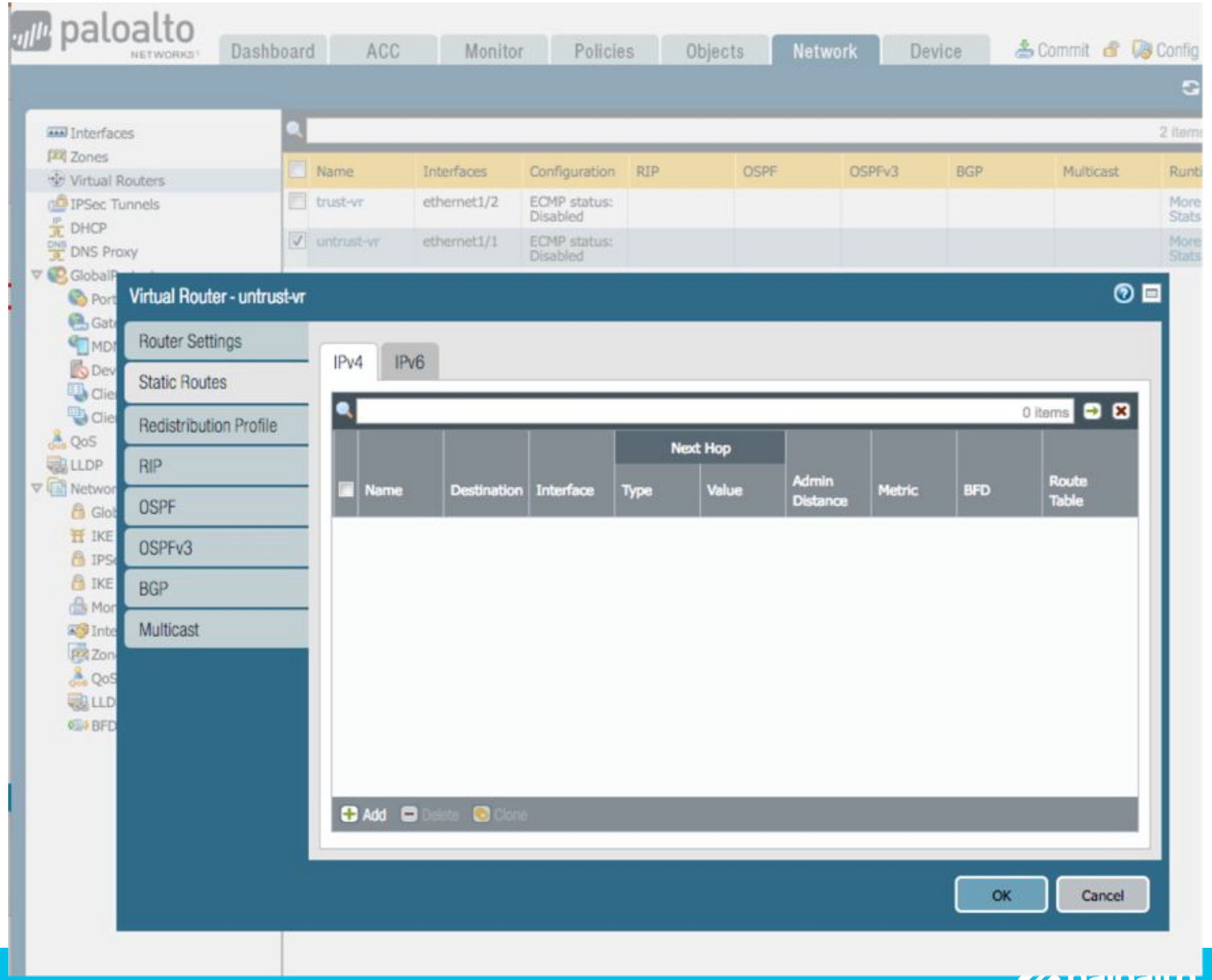


Configure Trust VR

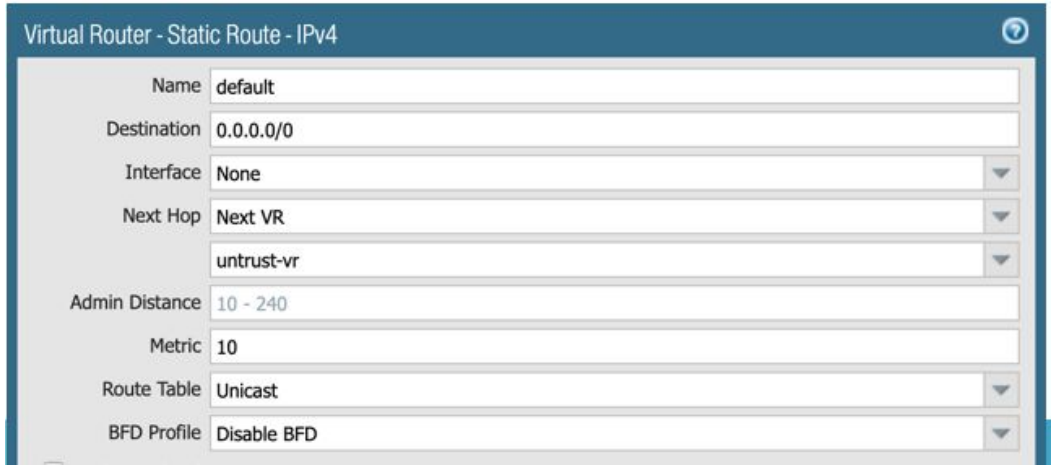
Go to:

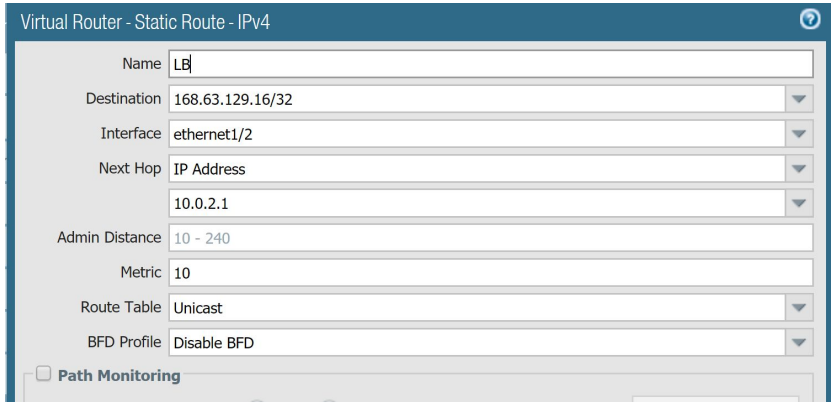
Network → Virtual Routers → **trust-vr**

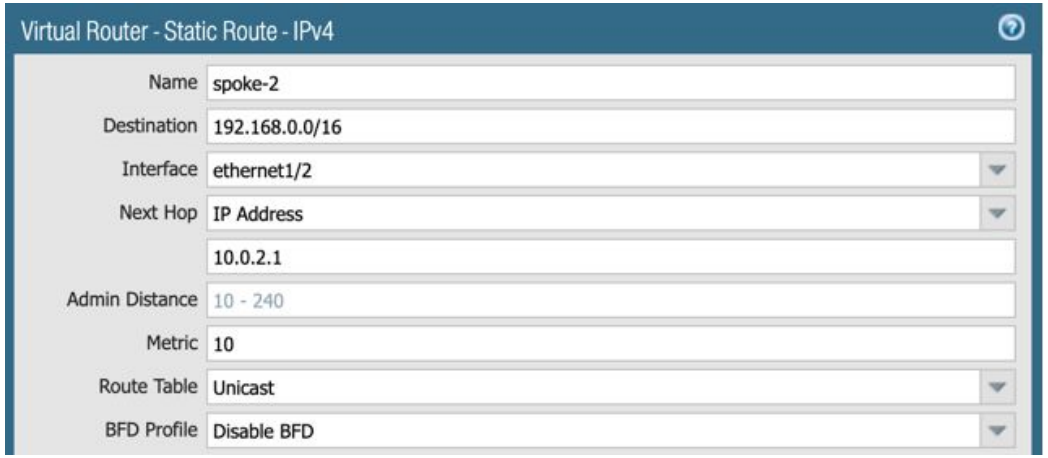
→ Static Routes → Add



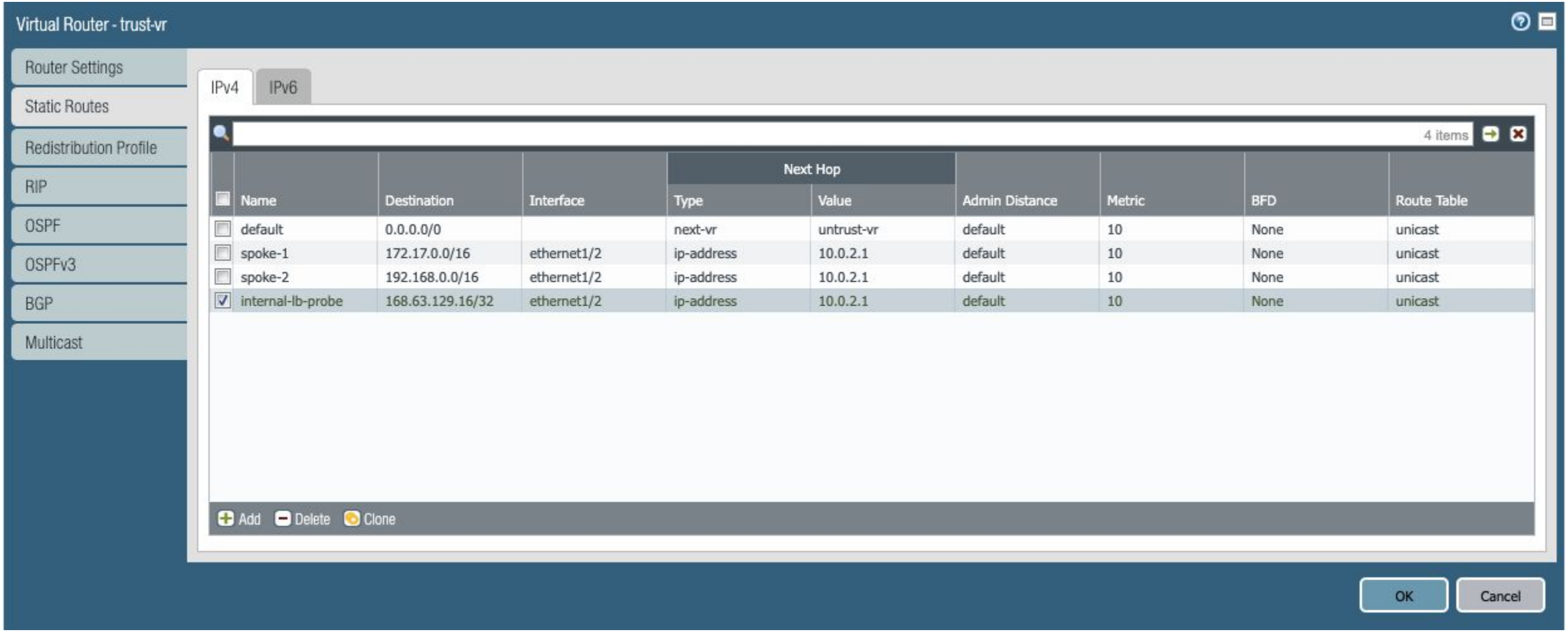
Configure Trust VR - Static Routes







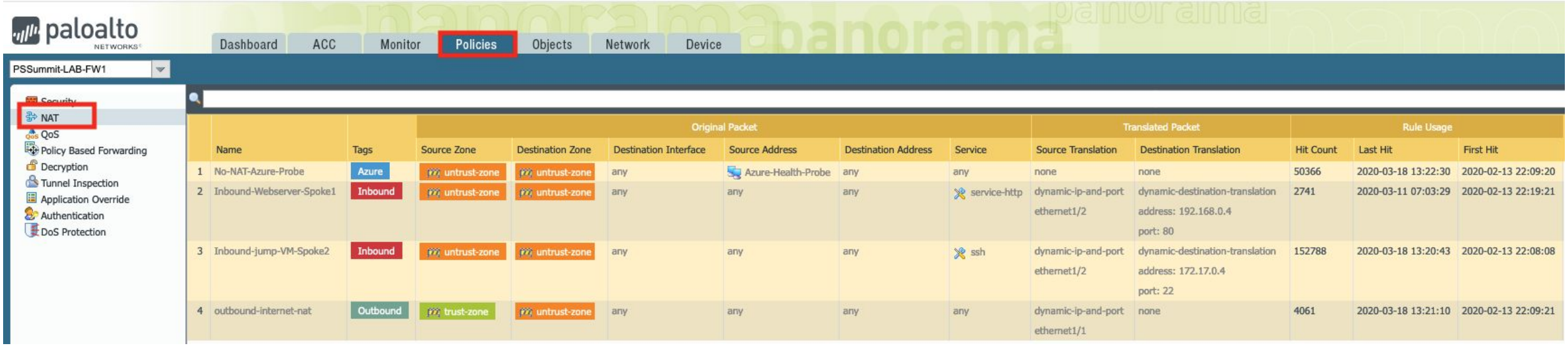
Configure Trust VR - Static Routes



Repeat these steps on FW2 using the same settings

Configure
NAT & Security Policies

NAT Policy Overview



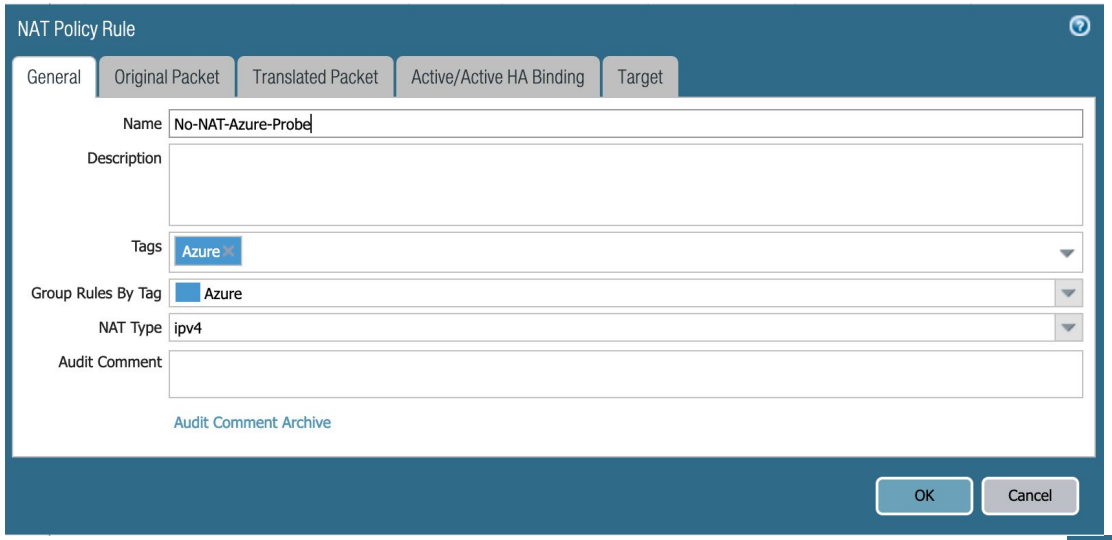
			Original Packet						Translated Packet		Rule Usage		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count	Last Hit	First Hit
1	No-NAT-Azure-Probe	Azure	untrust-zone	untrust-zone	any	Azure-Health-Probe	any	any	none	none	50366	2020-03-18 13:22:30	2020-02-13 22:09:20
2	Inbound-Webserver-Spoke1	Inbound	untrust-zone	untrust-zone	any	any	any	service-http	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 192.168.0.4 port: 80	2741	2020-03-11 07:03:29	2020-02-13 22:19:21
3	Inbound-jump-VM-Spoke2	Inbound	untrust-zone	untrust-zone	any	any	any	ssh	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 172.17.0.4 port: 22	152788	2020-03-18 13:20:43	2020-02-13 22:08:08
4	outbound-internet-nat	Outbound	trust-zone	untrust-zone	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	4061	2020-03-18 13:21:10	2020-02-13 22:09:21

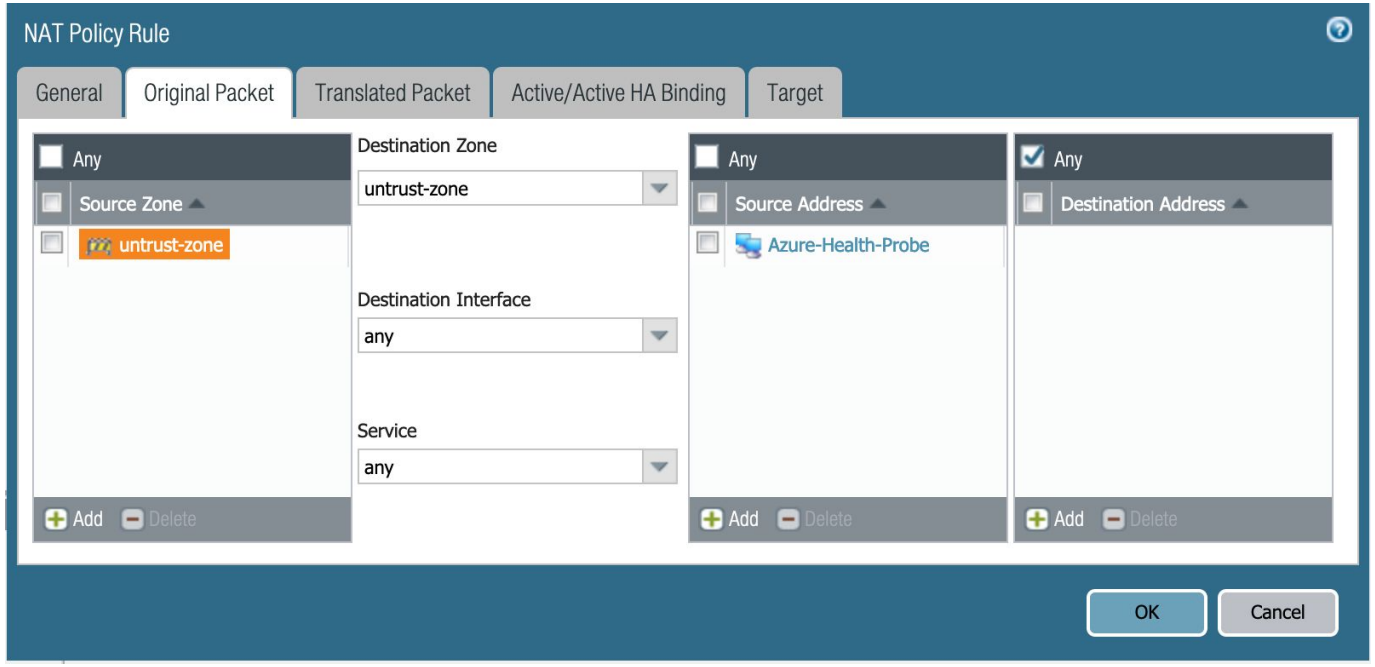
We need to create four NAT Policies:

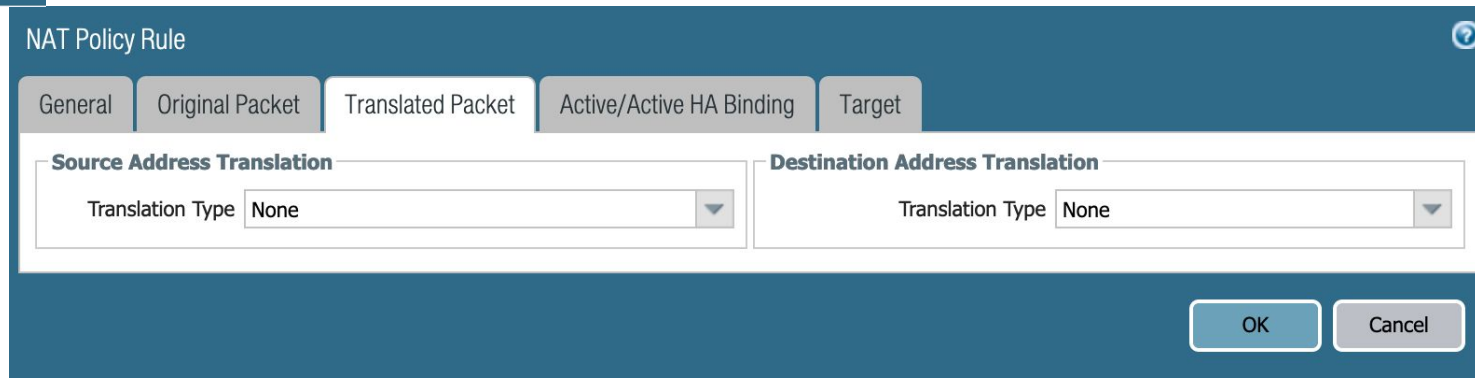
1. No-NAT-Azure-Probe
2. Inbound-WebServer-Spoke1
3. Inbound-Jump-VM-Spoke2
4. outbound-internet-nat

No NAT Policy for Azure Health Probe

Azure Health Probe IP: 168.63.129.16/32

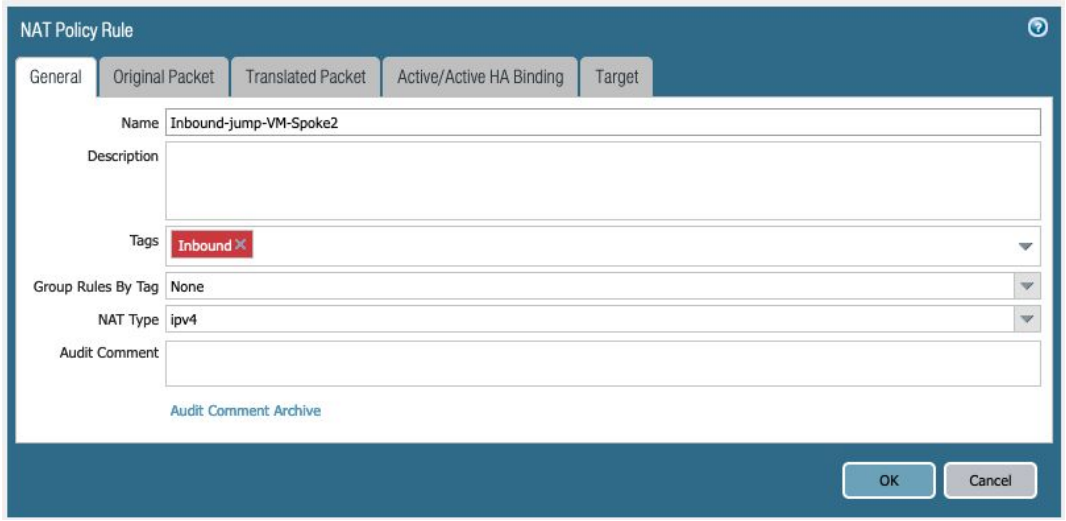


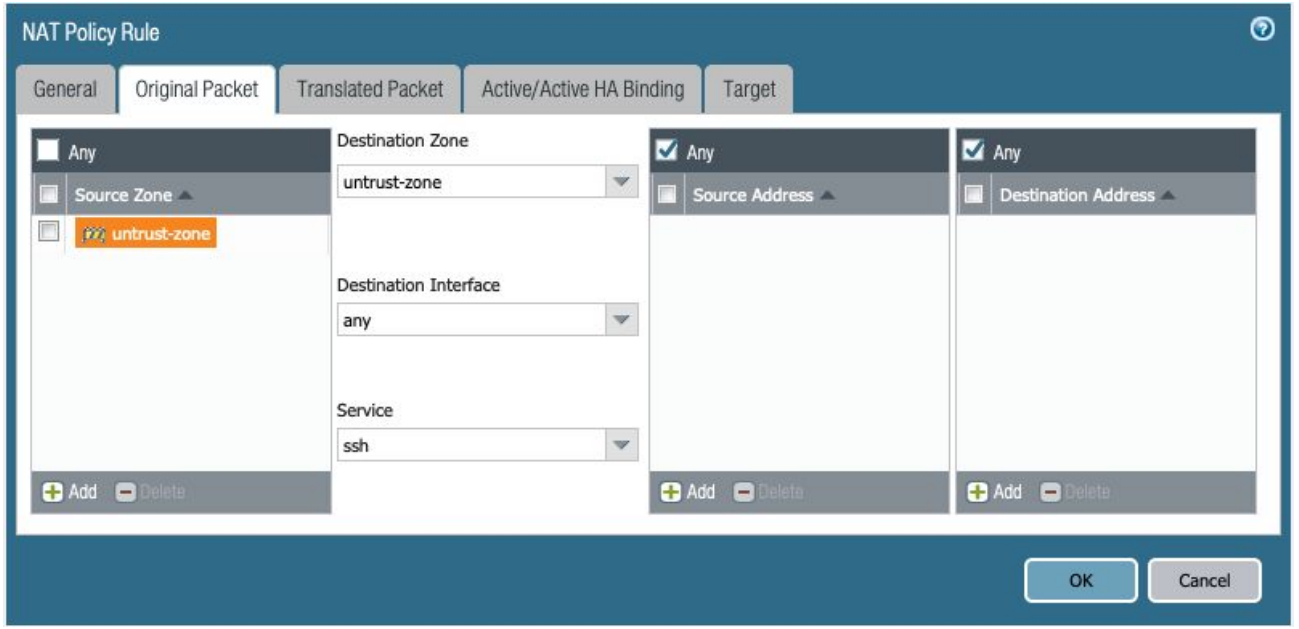


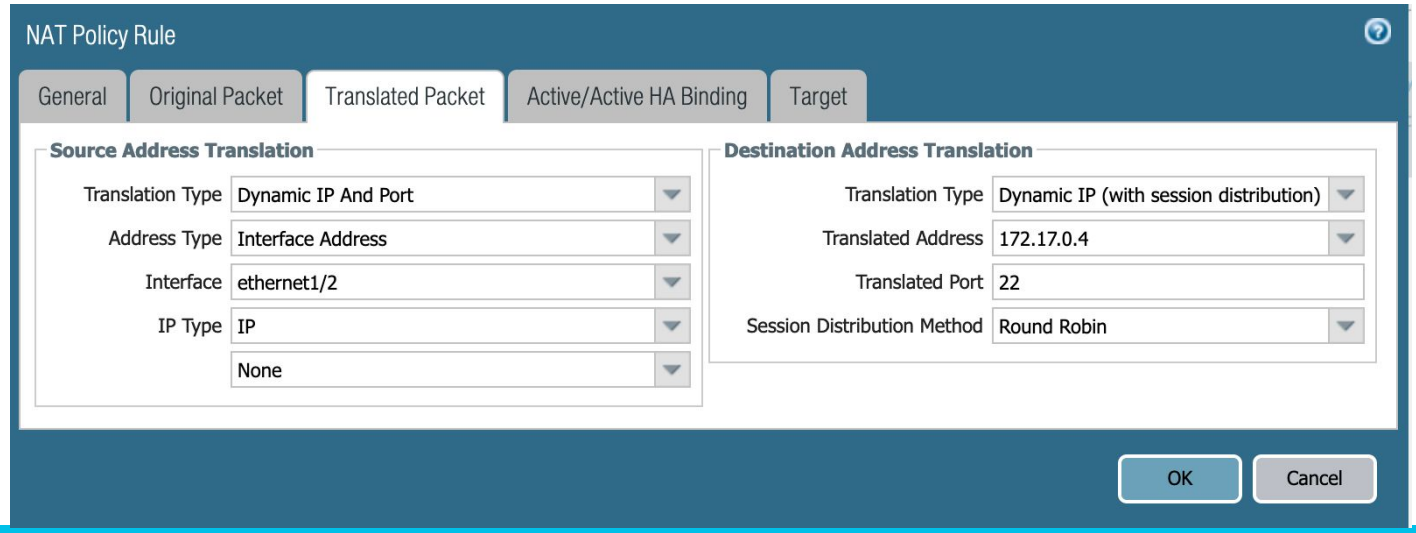


NAT Policy for VM Jumphost

The Destination address is the IP of the Untrust NIC of the Firewall

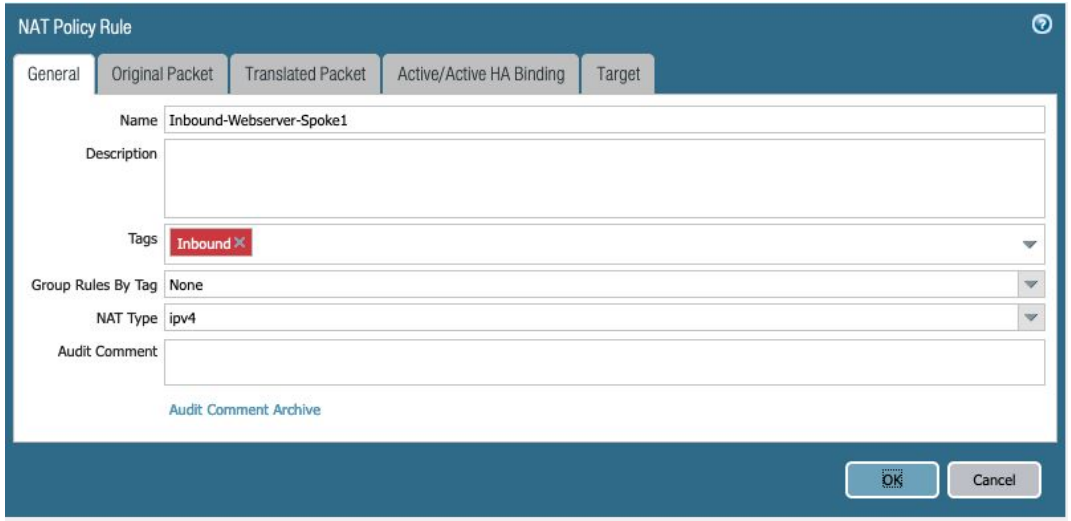


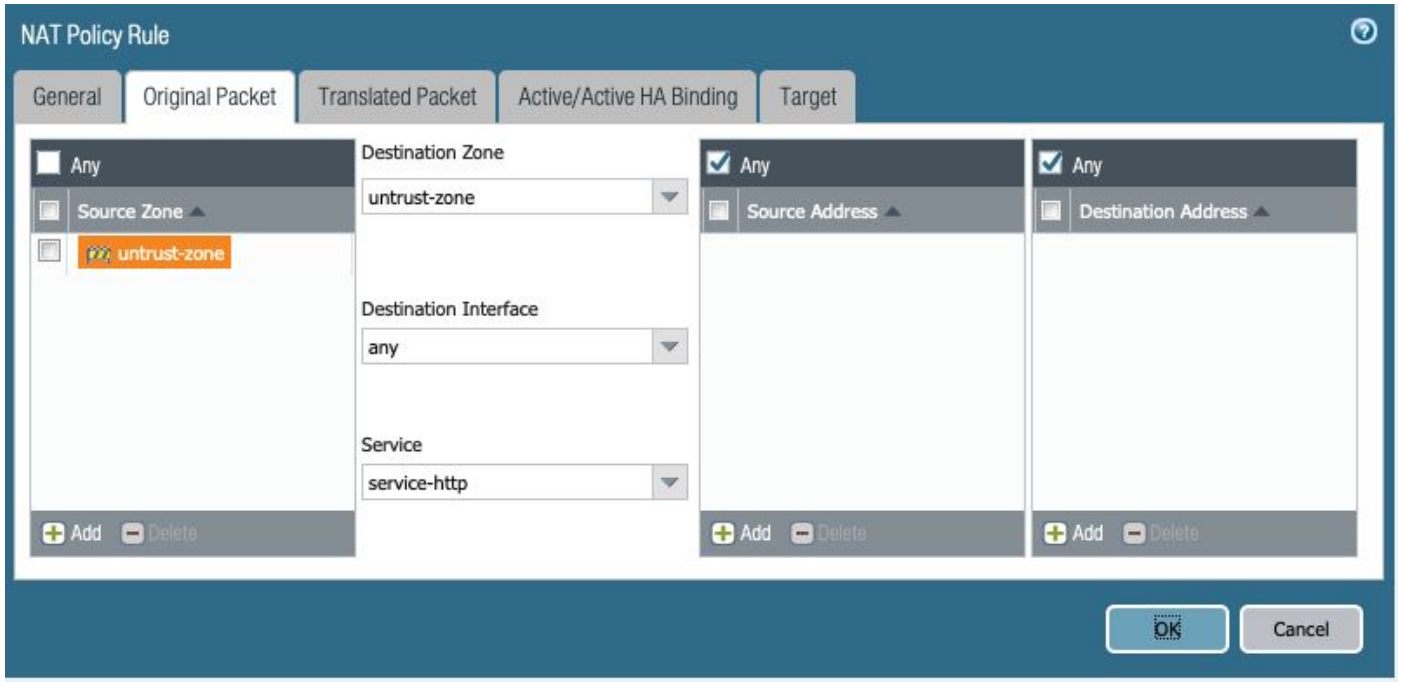


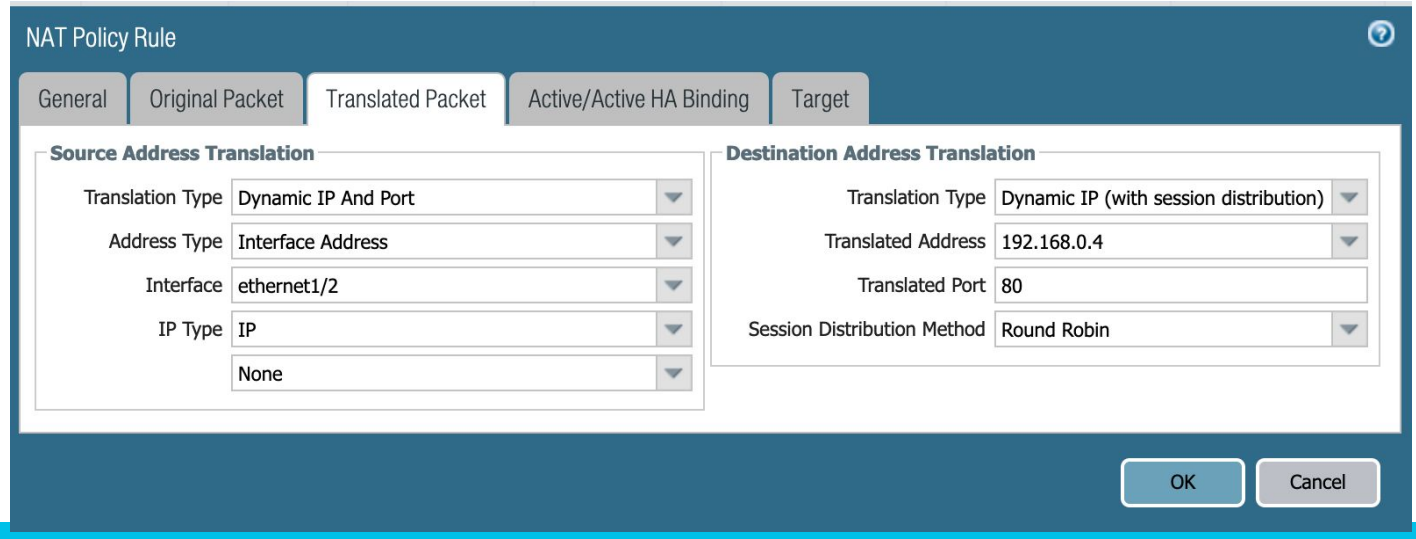


NAT Policy for the Webserver

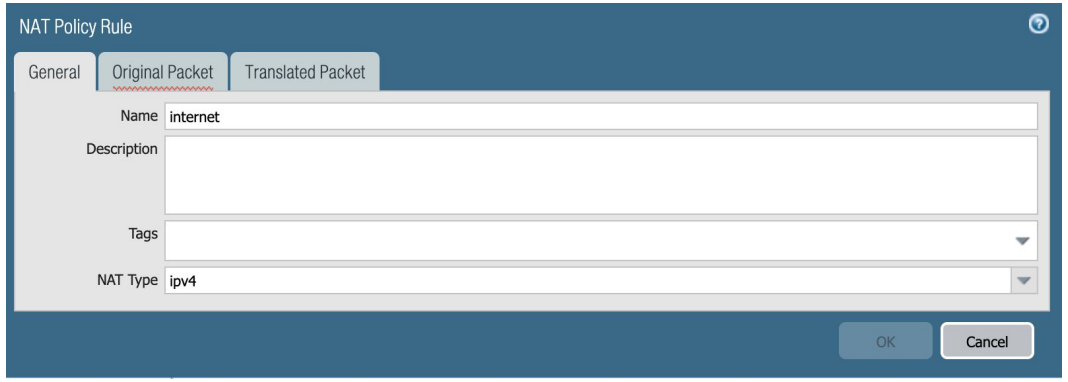
The Destination address is the IP of the Untrust NIC of the Firewall

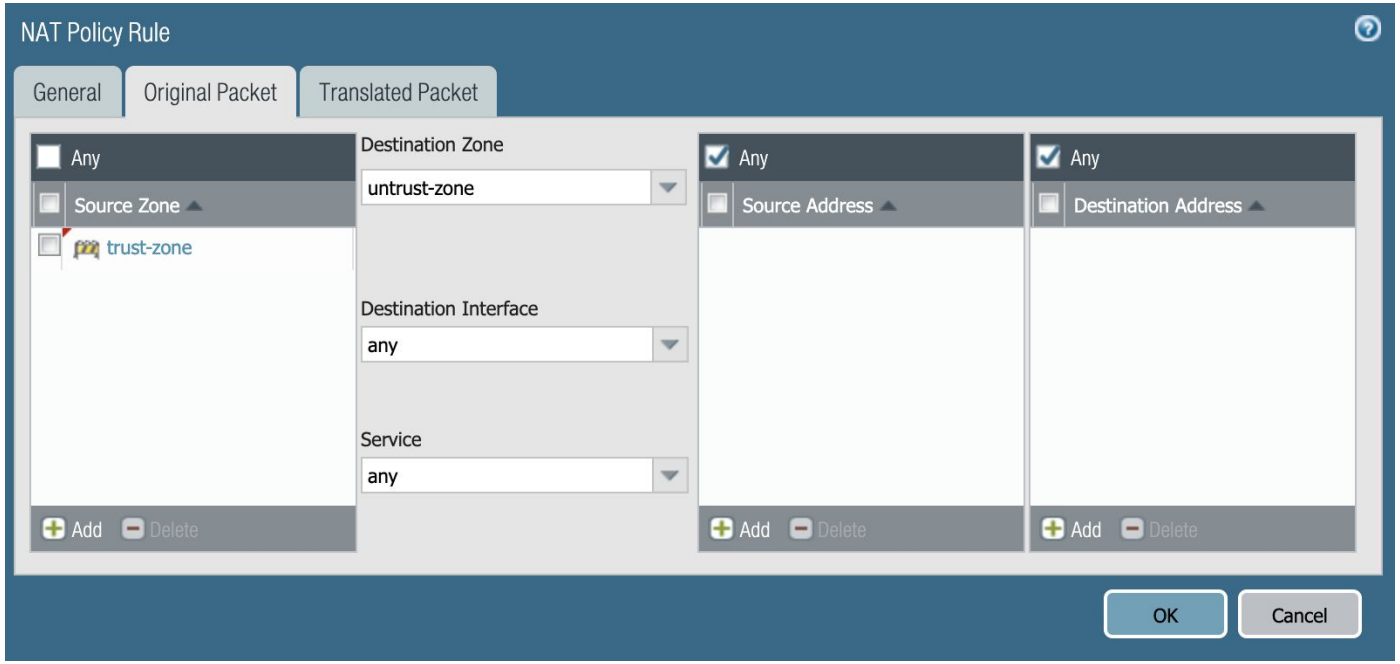


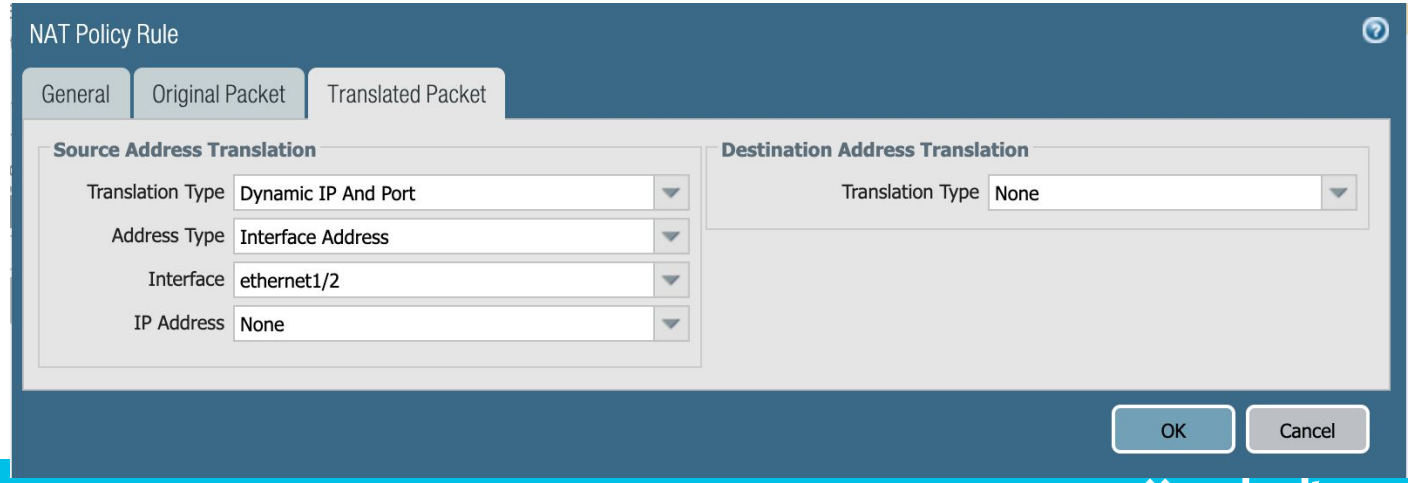




NAT Policy: outbound-internet-nat

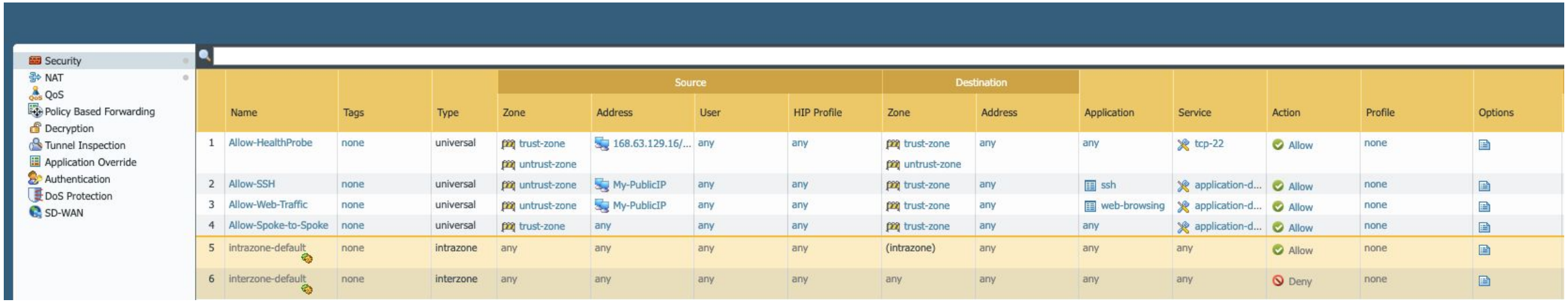






Create Limited Security rules

Replace “My-PublicIP” with your yours



	Name	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options
				Zone	Address	User	HIP Profile	Zone	Address					
1	Allow-HealthProbe	none	universal	trust-zone untrust-zone	168.63.129.16/...	any	any	trust-zone untrust-zone	any	any	tcp-22	Allow	none	
2	Allow-SSH	none	universal	untrust-zone	My-PublicIP	any	any	trust-zone	any	ssh	application-d...	Allow	none	
3	Allow-Web-Traffic	none	universal	untrust-zone	My-PublicIP	any	any	trust-zone	any	web-browsing	application-d...	Allow	none	
4	Allow-Spoke-to-Spoke	none	universal	trust-zone	any	any	any	trust-zone	any	any	application-d...	Allow	none	
5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	
6	interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	

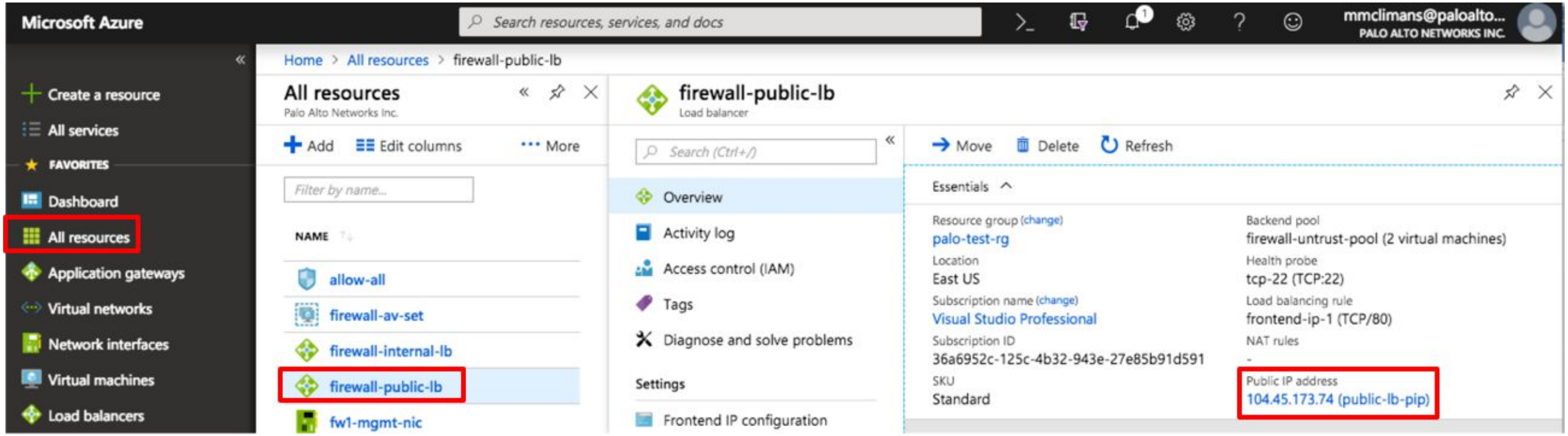
Repeat these steps on FW2 using the same settings

Commit your changes

TEST TRAFFIC FLOWS

Find Public LB Public IP

1. Go to the Azure Portal → All Resources → Your Resource Group → firewall-public-lb
2. Copy the public IP associated with Public Load Balancer



SSH into the Jump Host

Open an SSH session using the hostname, username, and password below.

Hostname: Your-Public-LB-IP

```
AMSMACF1WWG8WL:~ tostern$ ssh ubuntu@192.168.0.4
```

Try to pinging to the Internet

```
paloalto@jump-vm:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=2.72 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=3.21 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=3.21 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=3.09 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=116 time=2.81 ms
```

Try to pinging to the other spoke VM

```
paloalto@jump-vm:~$ ping 192.168.0.4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_seq=1 ttl=63 time=4.16 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=63 time=1.65 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=63 time=1.51 ms
```

SSH into Web VM and install Apache

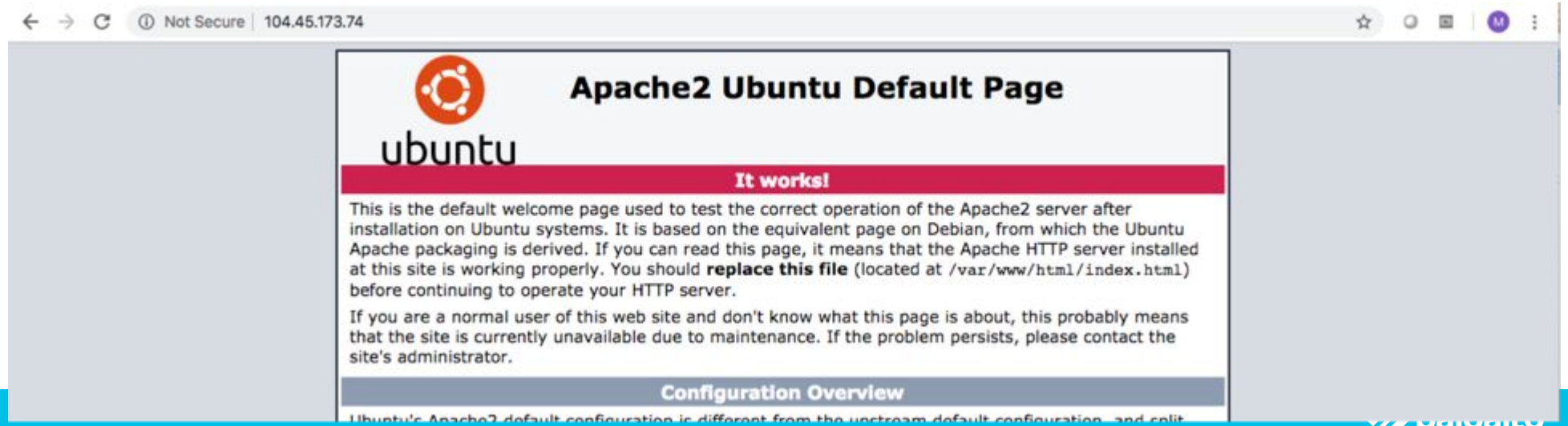
While in the jump-vm, SSH to the Web-VM in Spoke-2-VNET

```
paloalto@jump-vm:~$ ssh paloalto@192.168.0.4
```

Install apache by entering sudo apt-get install apache2

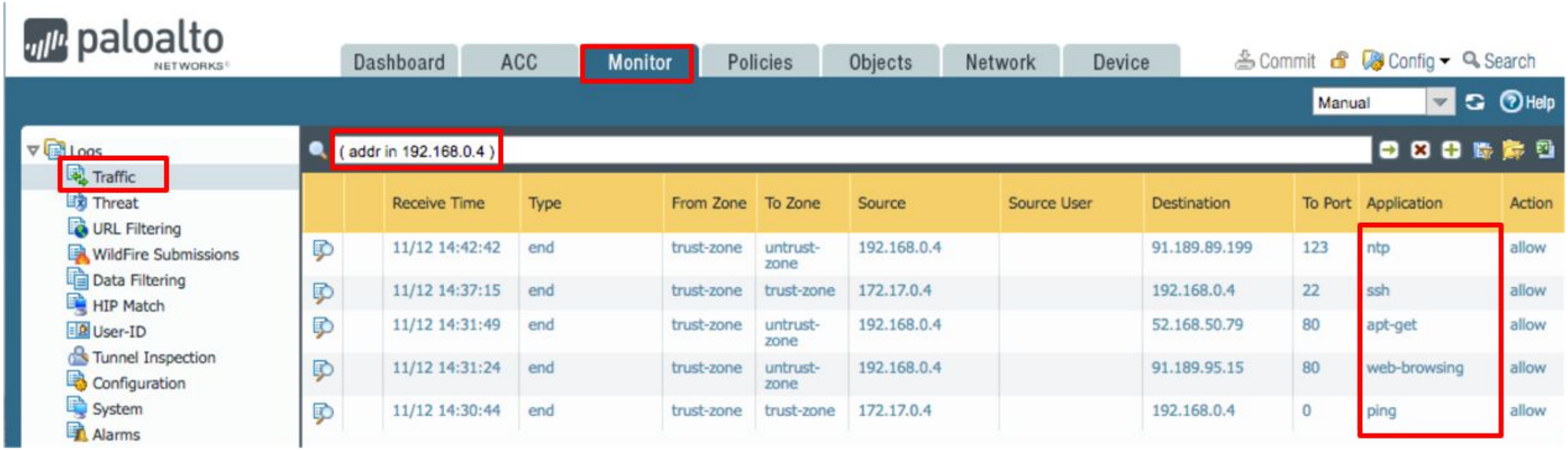
```
paloalto@web-vm:~$ sudo apt-get install apache2 -y
```

Paste the Public Load Balancers IP into your browser (i.e. http://<your-ip-here>) and a Apache page should open.



Filter Firewall Traffic Logs for your tested Traffic

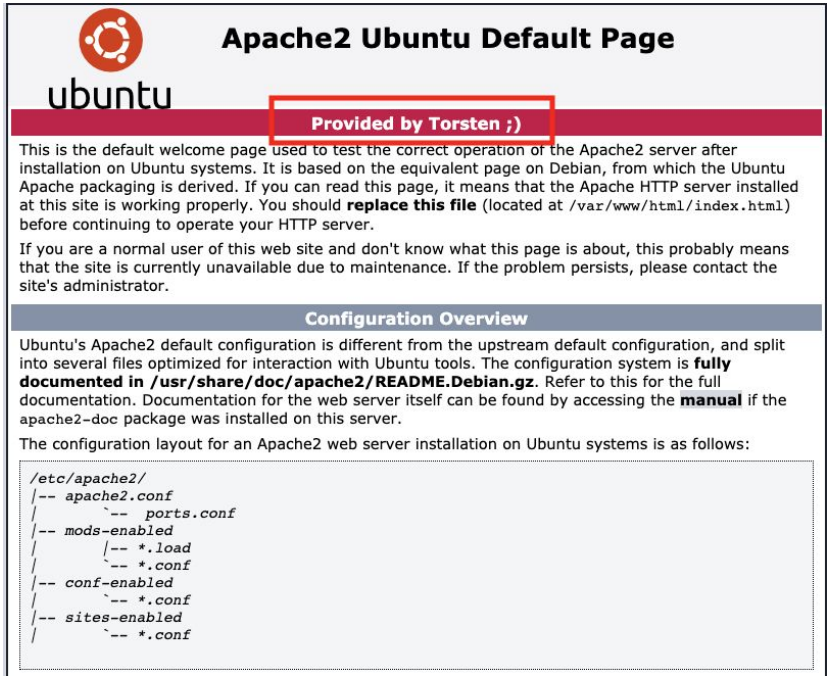
- Go to the firewall. Click Monitor → Traffic.
- Type the filter (addr in 192.168.0.4)to view all traffic associated with your web server.



If you do not see the logs, Check FW2 or check if you are searching for the correct address

Lab Completed

- Change the header in the Apache index.html file to your name



Hint ;)

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

Q&A

PRISMA
BY PALO ALTO NETWORKS
paloalto NETWORKS