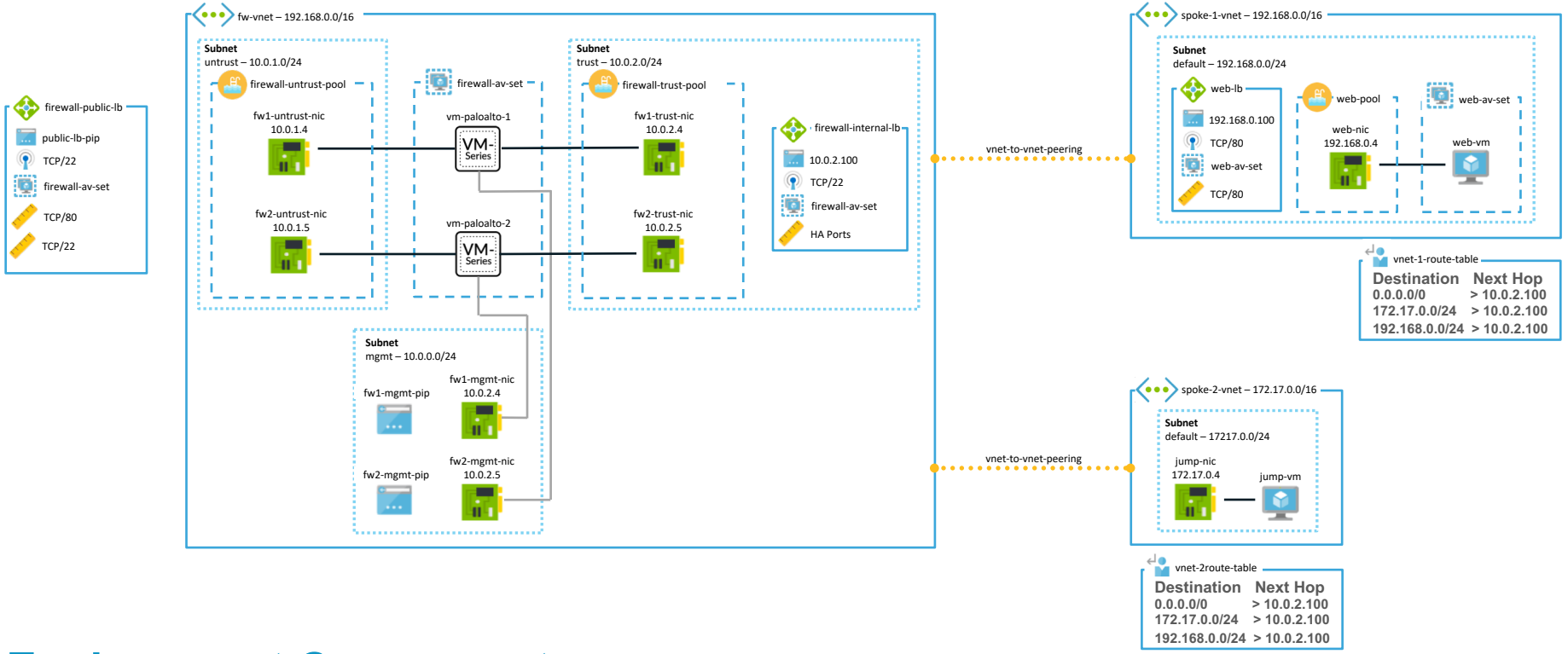
TRANSIT DEMO GUIDE

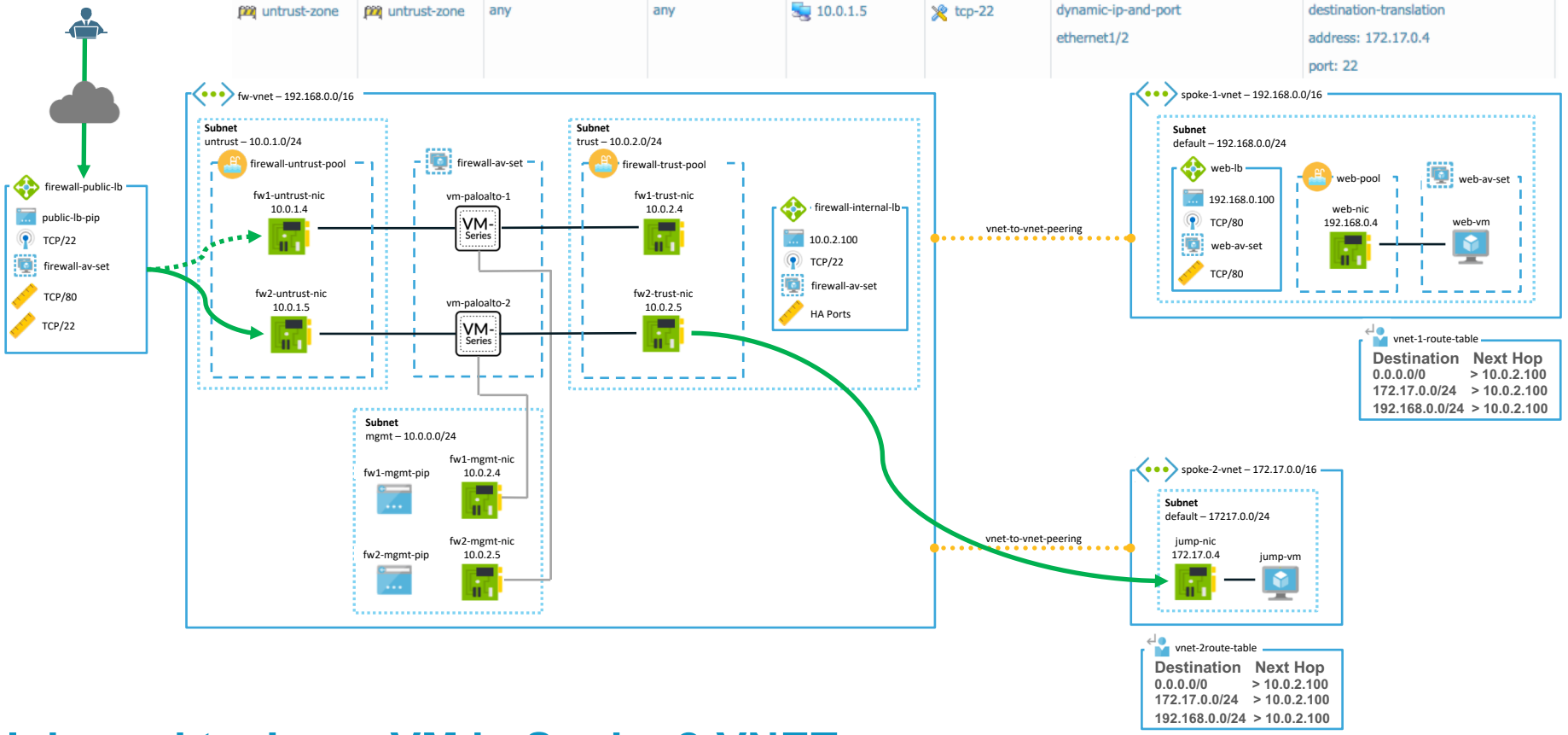
Matt McLimans, Public Cloud Consultant Engineer

paloalto NETWORKS®



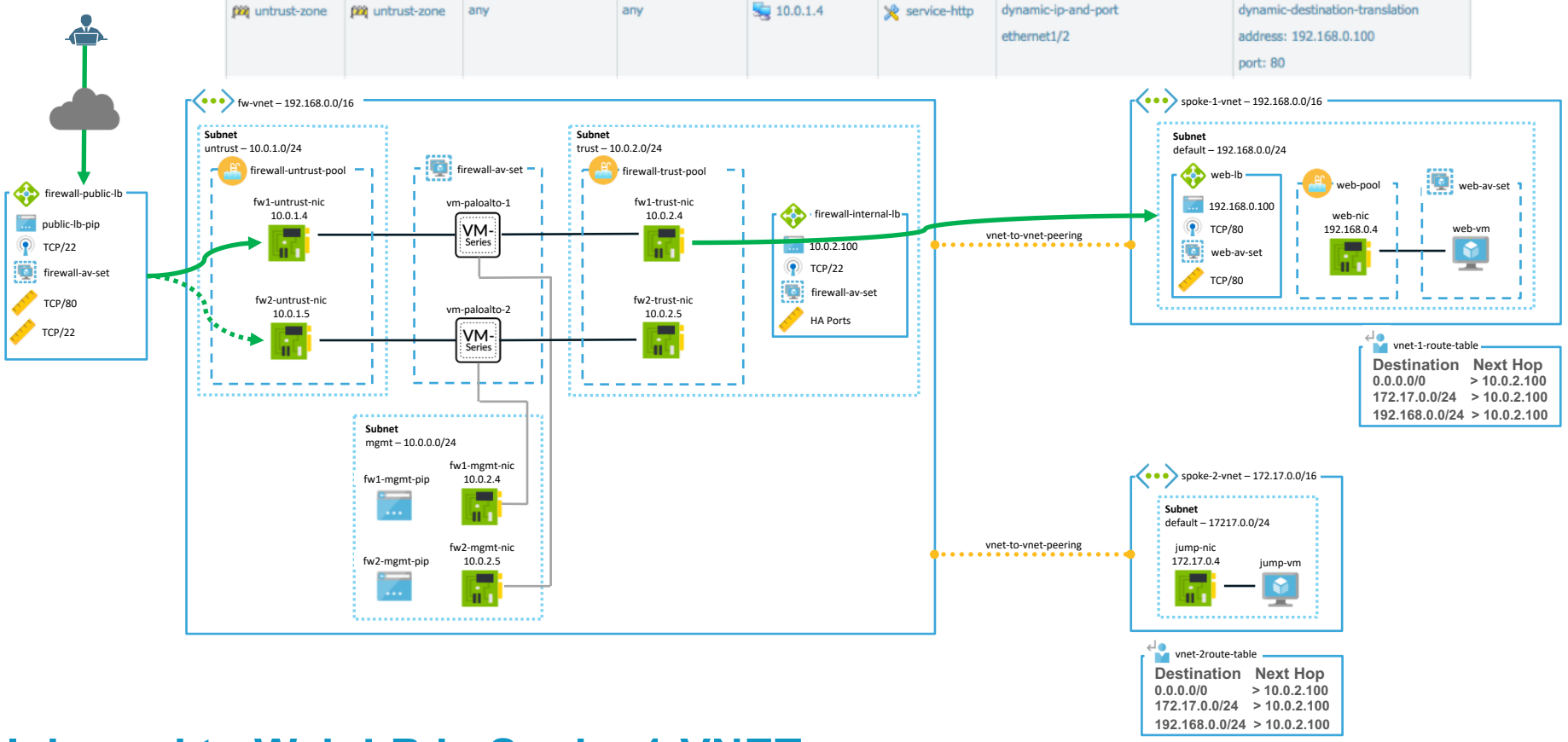
Environment Components

Original Packet						Translated Packet	
Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
untrust-zone	untrust-zone	any	any	10.0.1.5	tcp-22	dynamic-ip-and-port ethernet1/2	destination-translation address: 172.17.0.4 port: 22



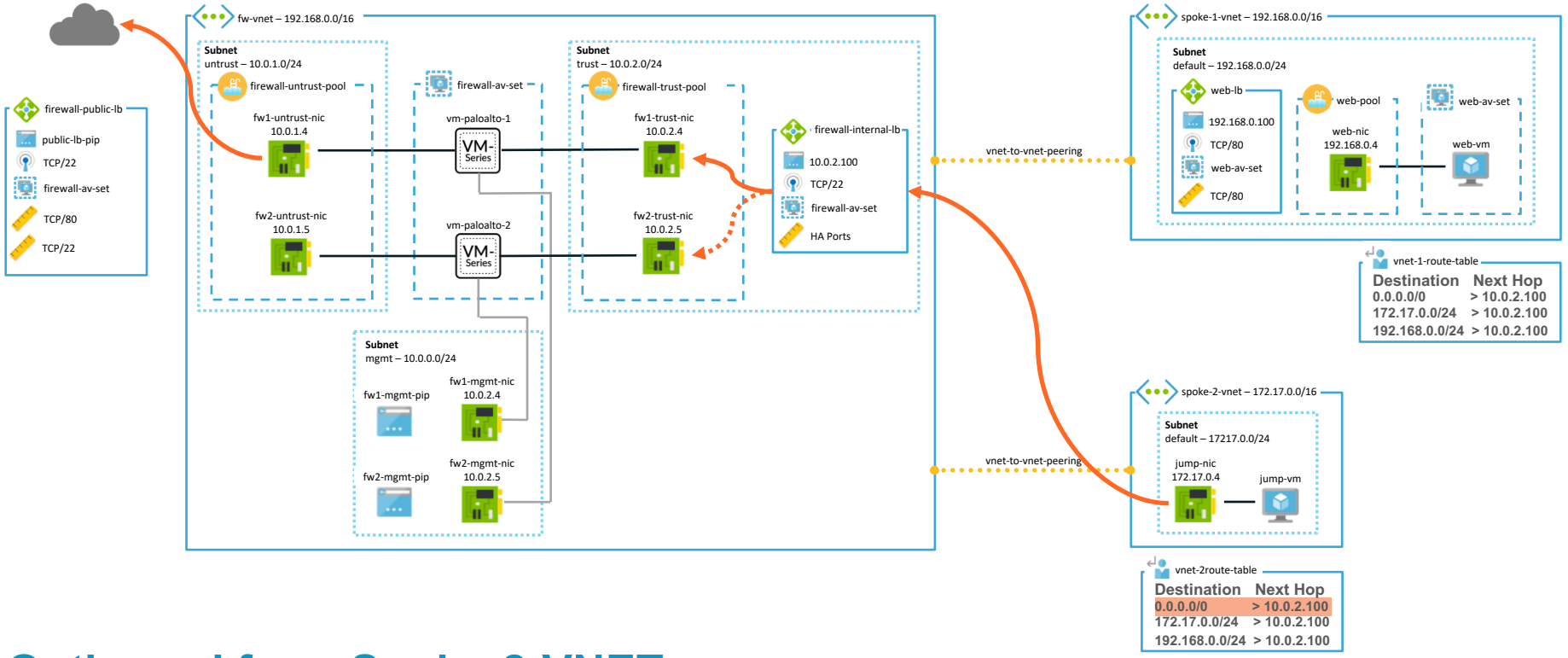
Inbound to Jump-VM in Spoke-2-VNET

Original Packet						Translated Packet	
Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
untrust-zone	untrust-zone	any	any	10.0.1.4	service-http	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 192.168.0.100 port: 80

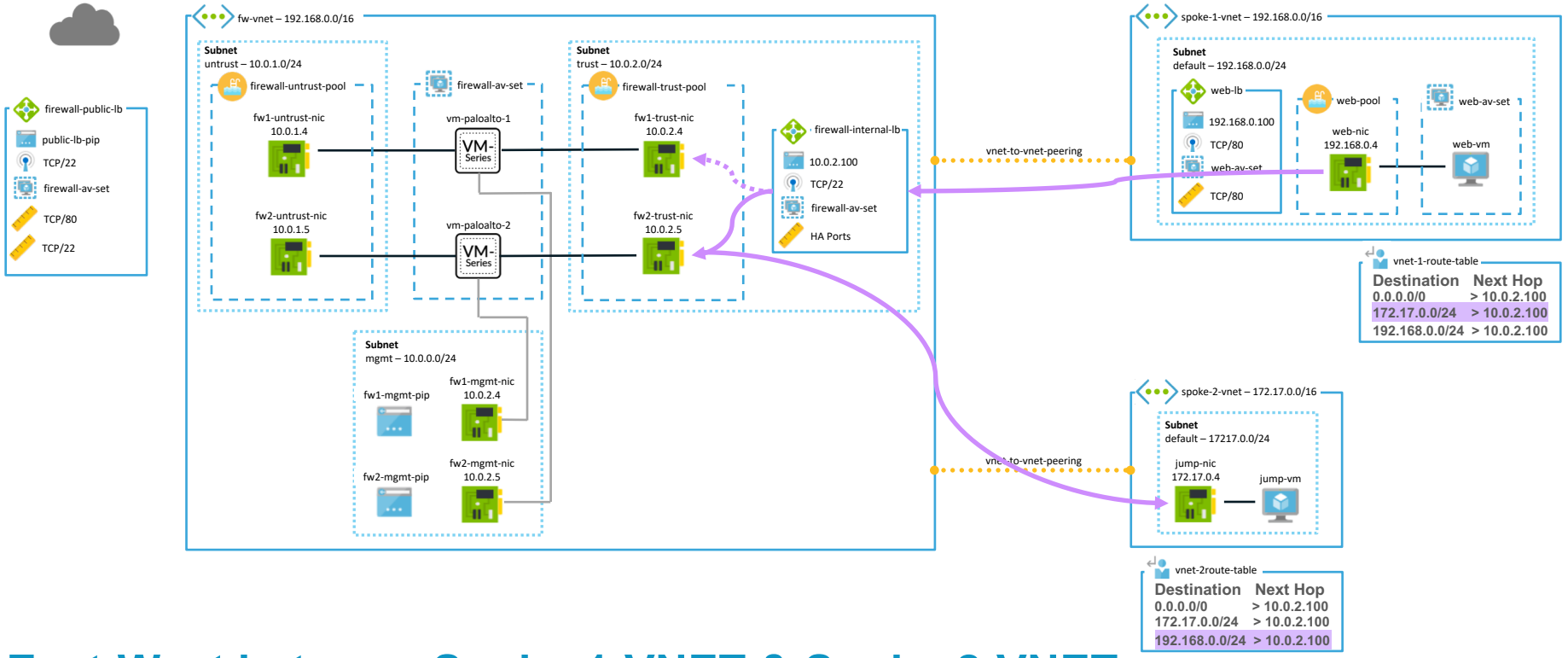


Inbound to Web LB in Spoke-1-VNET

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



Outbound from Spoke-2-VNET



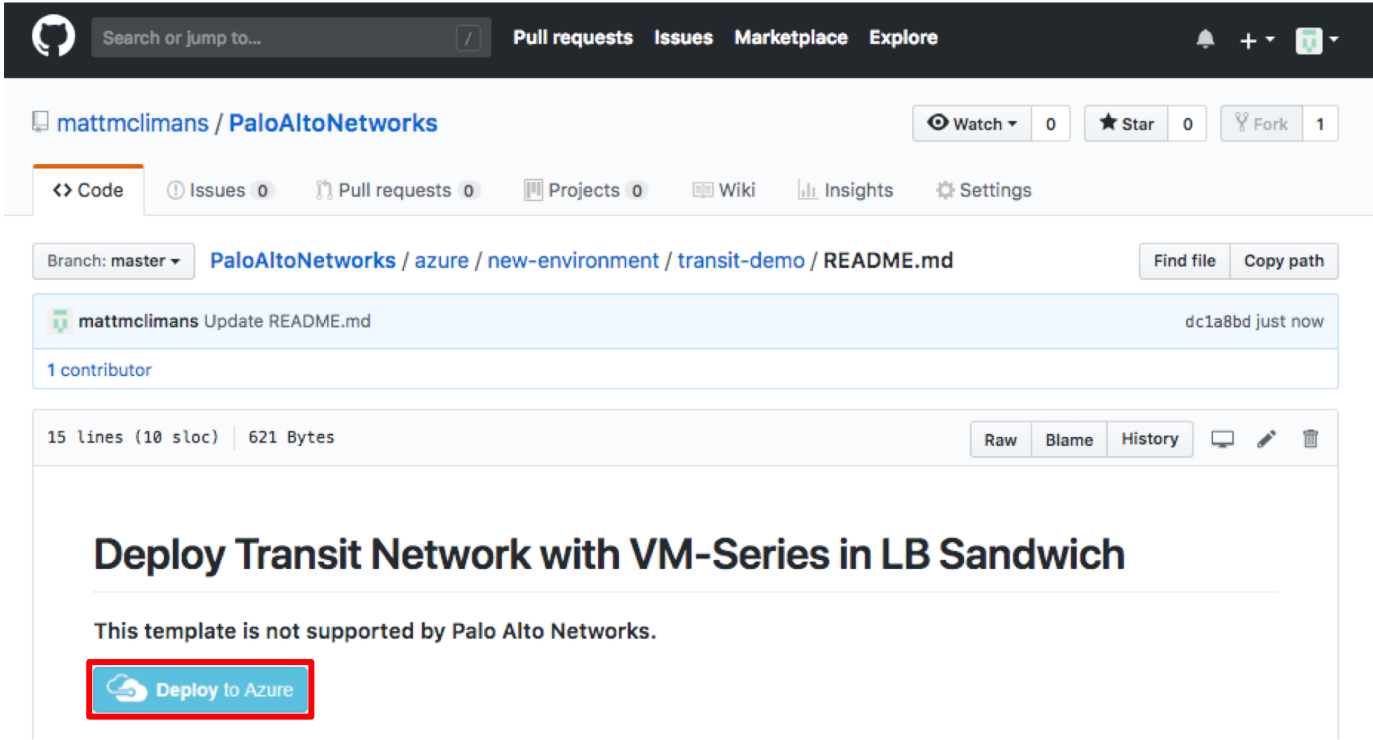
East-West between Spoke-1-VNET & Spoke-2-VNET

Deploy the Template

Step A1. Launch the Template

1. Go to: https://github.com/mattmclimans/PaloAltoNetworks/tree/master/azure/new-environment/transit-demo

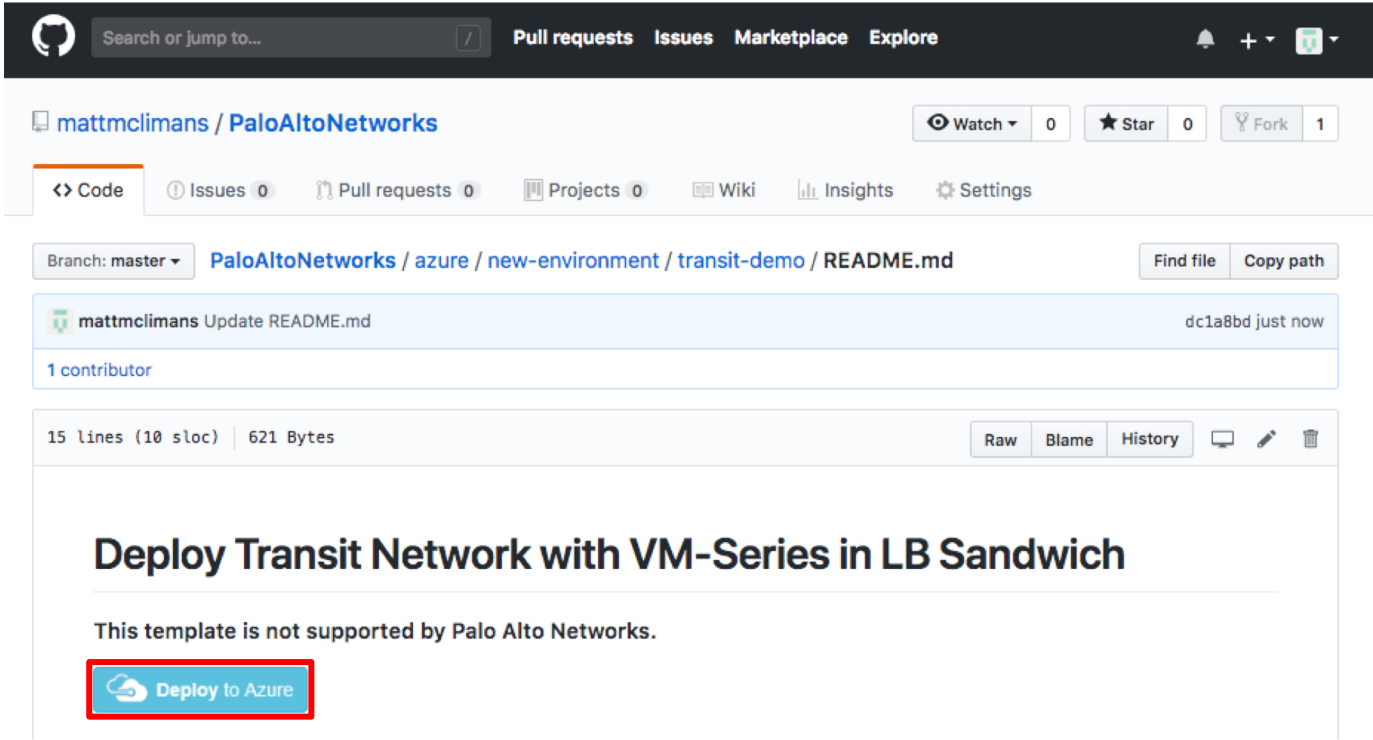
2. Click “Deploy to Azure”



Step A2. Setup Auth Codes

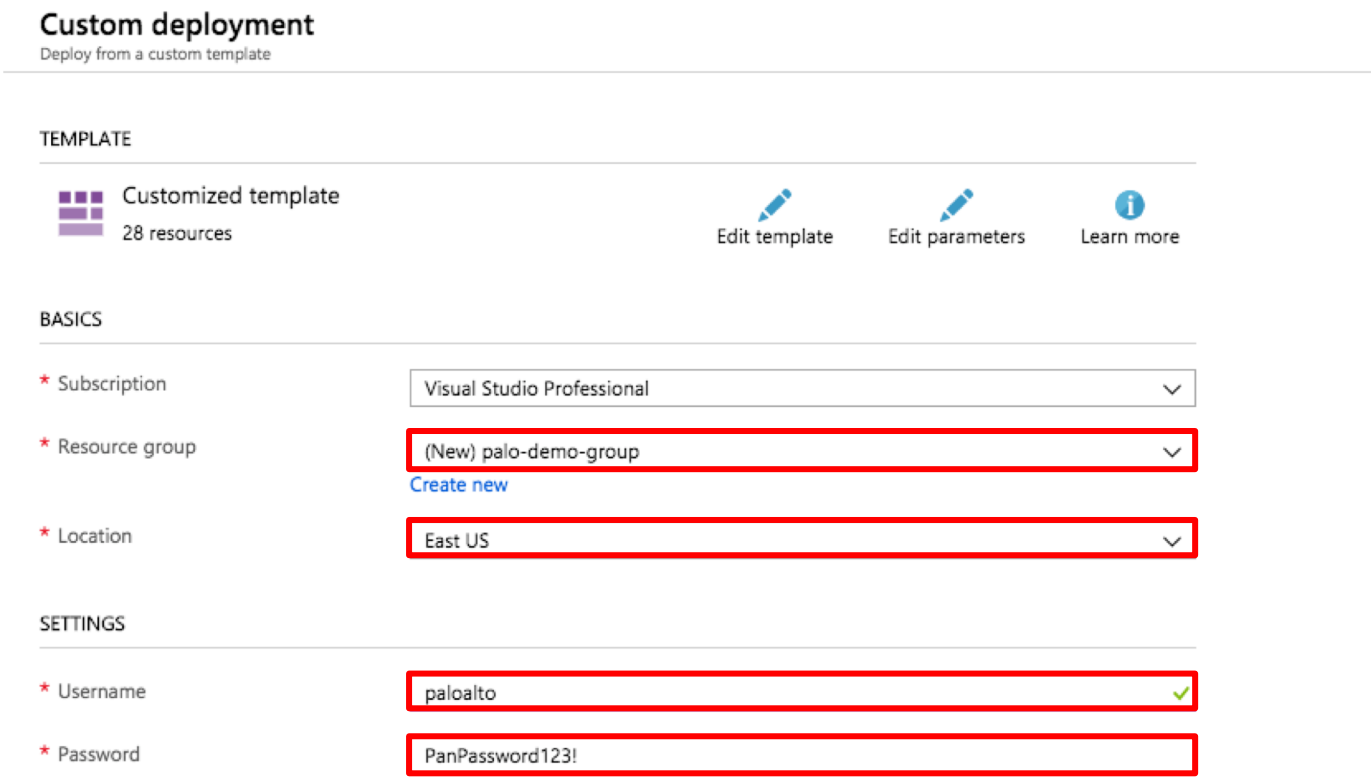
1. Go to: https://support.paloaltonetworks.com

2. Click “Deploy to Azure”



Step A3. Create New Resource Group

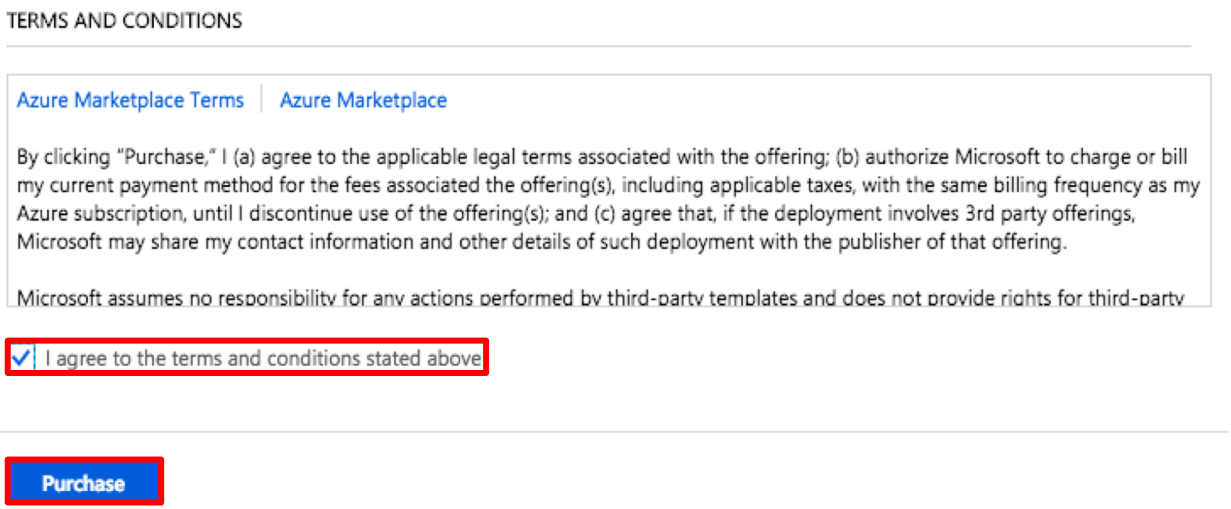
1. Create a new Resource Group.
2. Select East US for the region.



Step A4. Agree to Terms & Conditions

1. Scroll to bottom
2. Accept Licensing Terms and Conditions
3. Click Purchase

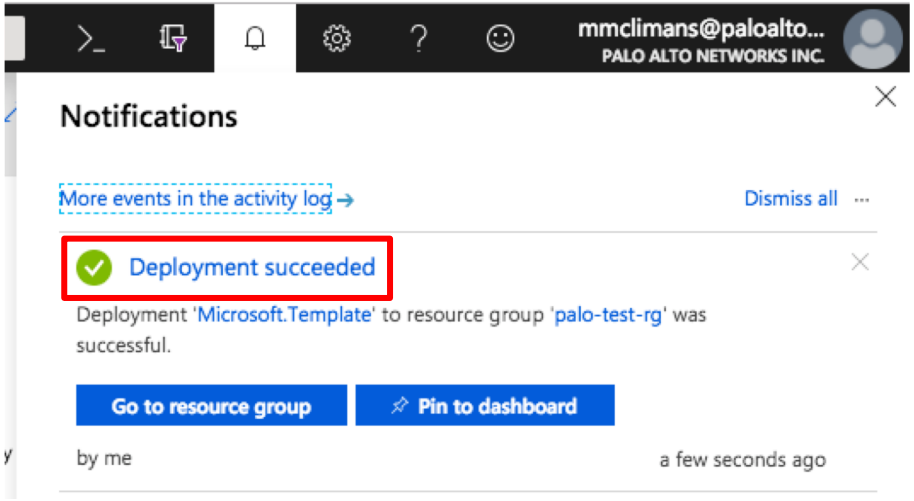
DO NOT CHANGE ANY OTHER FIELDS.



Step A5. Wait for deployment to complete…

Deployment takes ~10 Minutes to complete.

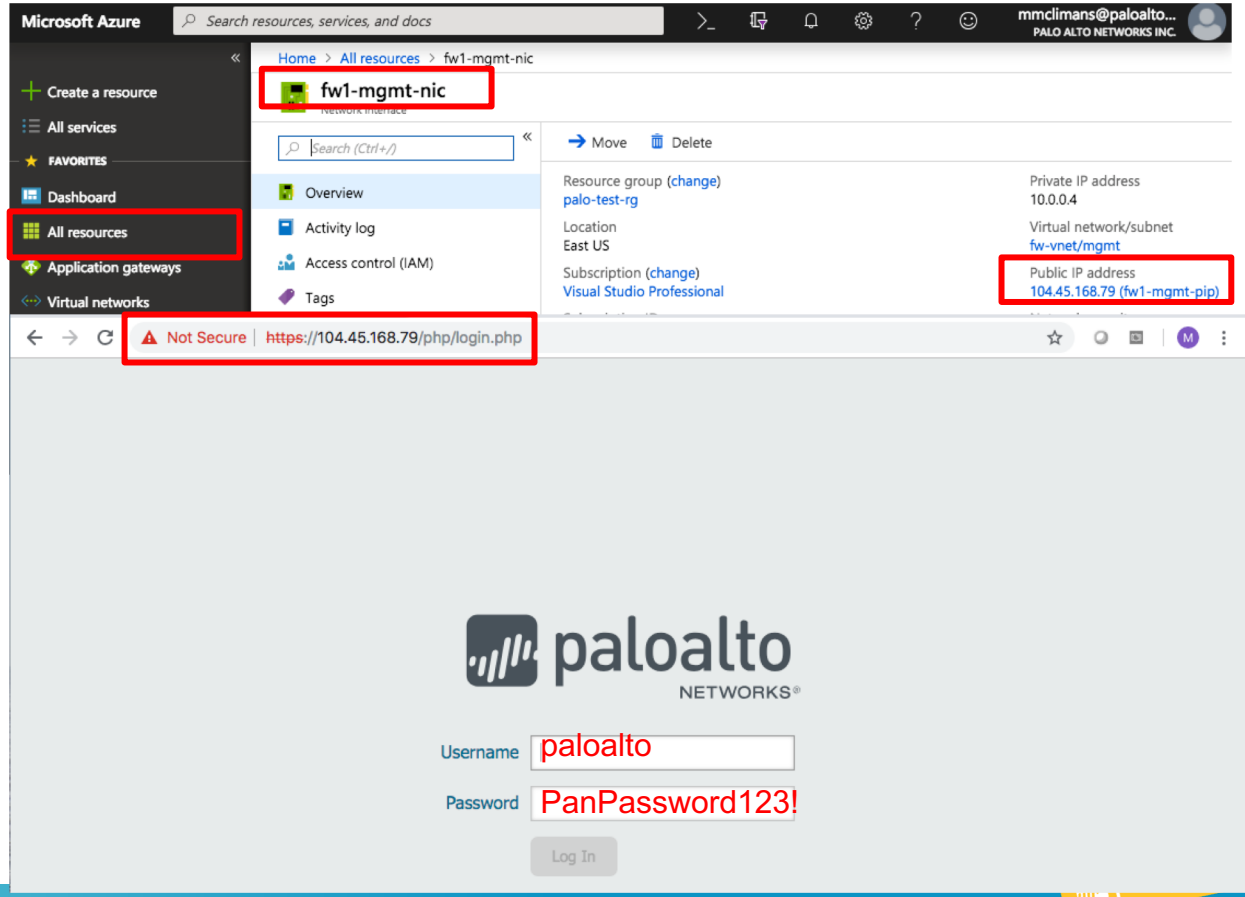
Once the template finishes, the bell in the top right corner will say "***Deployment Succeeded***"



License the Firewall

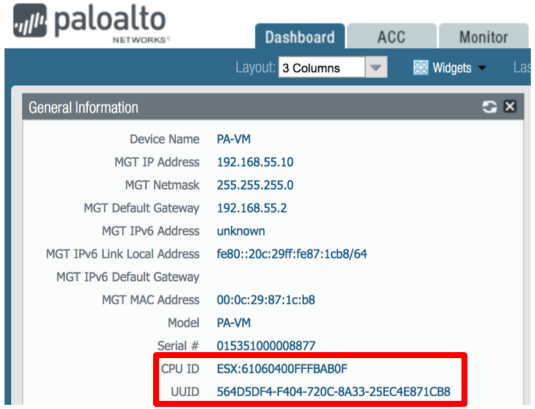
Step B1. Find FW-1 Management IP.

1. Go to All Resources→fw1-mgmt-pip
2. Copy the Public IP Address to your clipboard.
3. Paste the IP in a browser preceded by https://
4. Accept certificate warning and enter the credentials:
    1. Username: **paloalto**
    2. Password: **PanPassword123!**

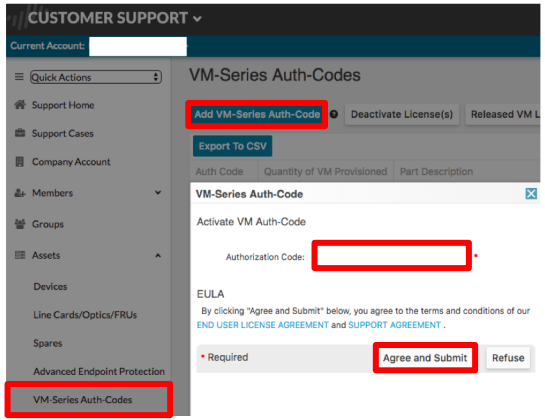


Step B2. License the VM-Series

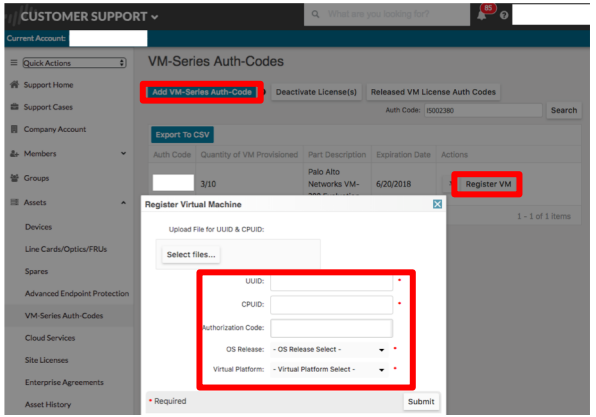
Step 1. Copy CPU ID & UUID from firewall dashboard.



Step 2. Go to https://support.paloaltonetworks.com
Assets→VM-Series Auth Codes→Add VM-Series Auth Code
Type your Authorization Code and click **Agree and Submit**

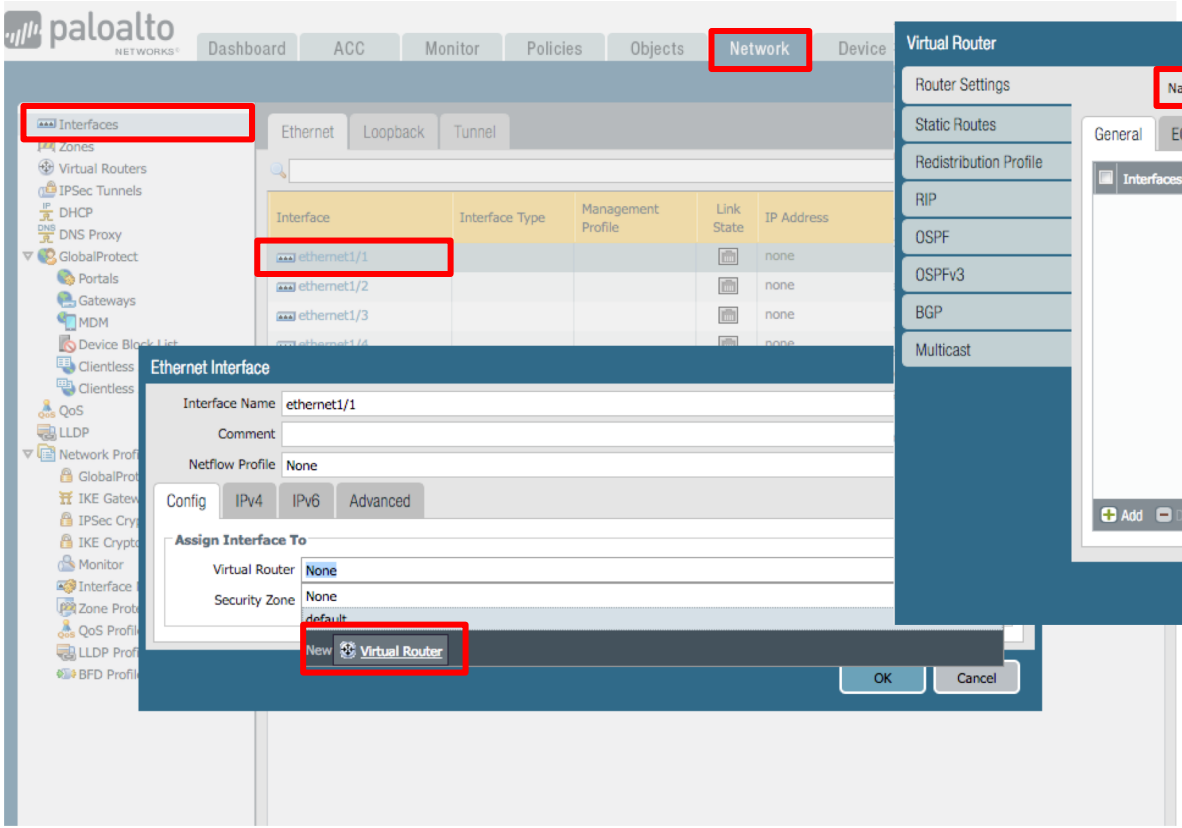


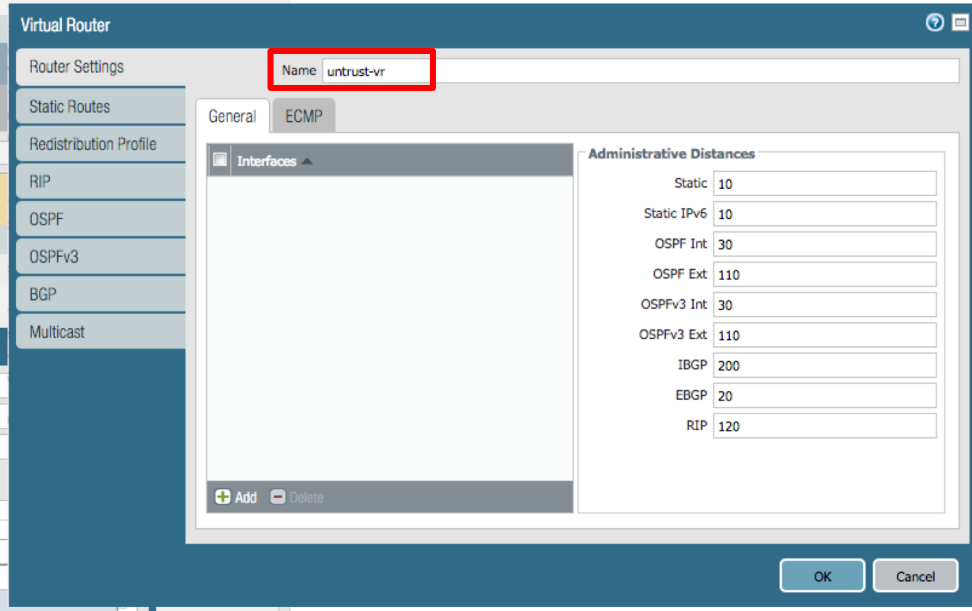
Step 3. Click **Register VM** next to your Auth Code
Paste your UUID and CPUID
Select OS Release and Virtual Platform (Azure)
Click **Submit**



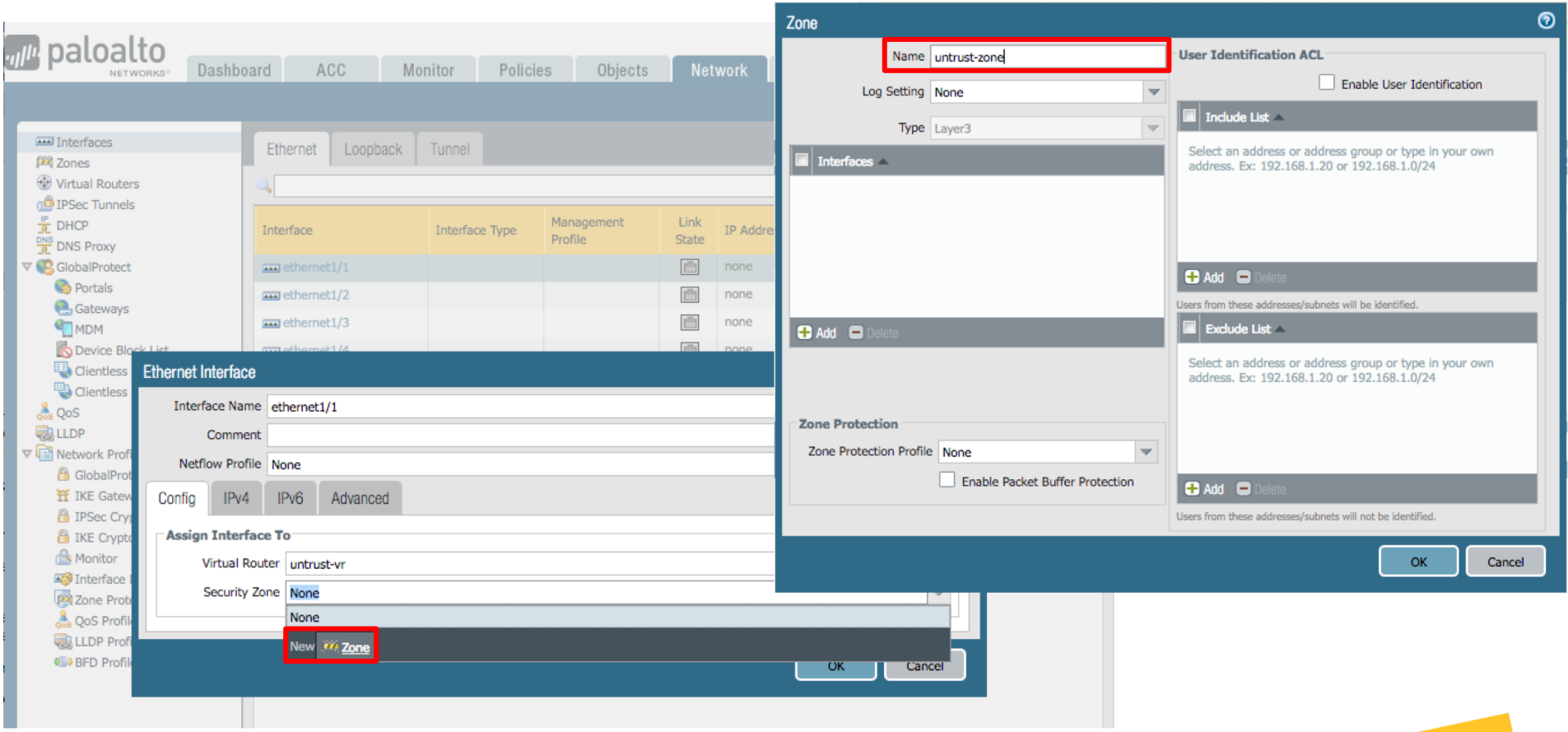
Configure Untrust and Trust NICs

Step B3. Assign Virtual Router to Ethernet1/1



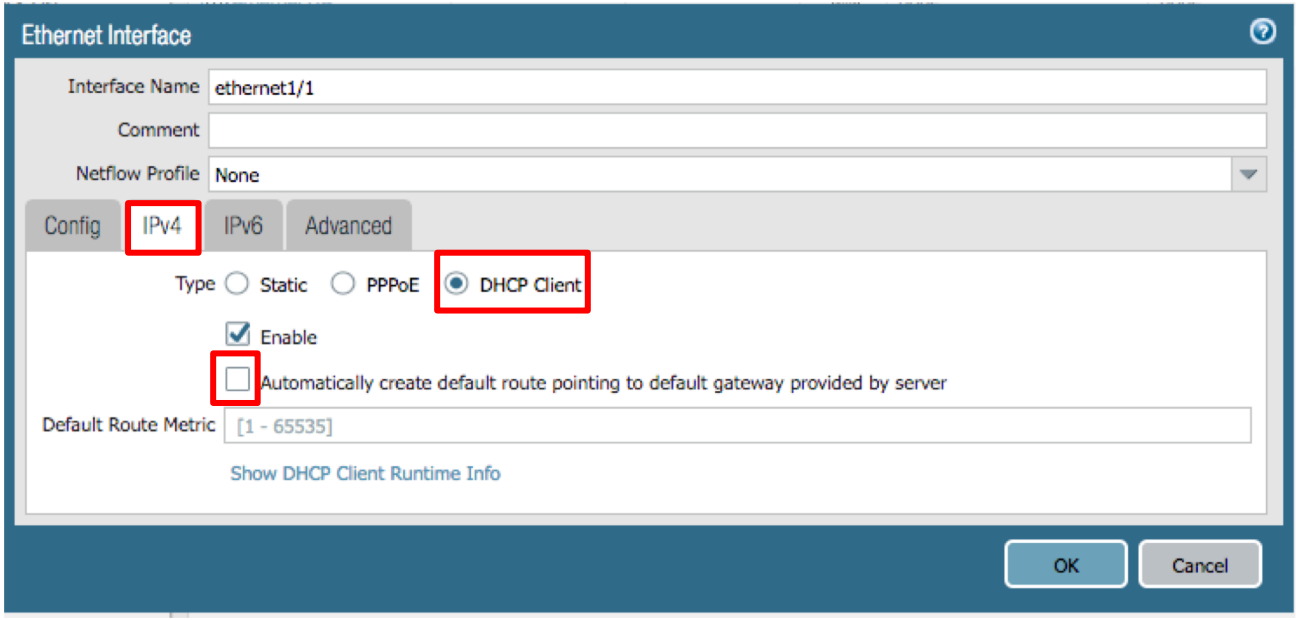


Step B4. Assign Zone to Ethernet1/1



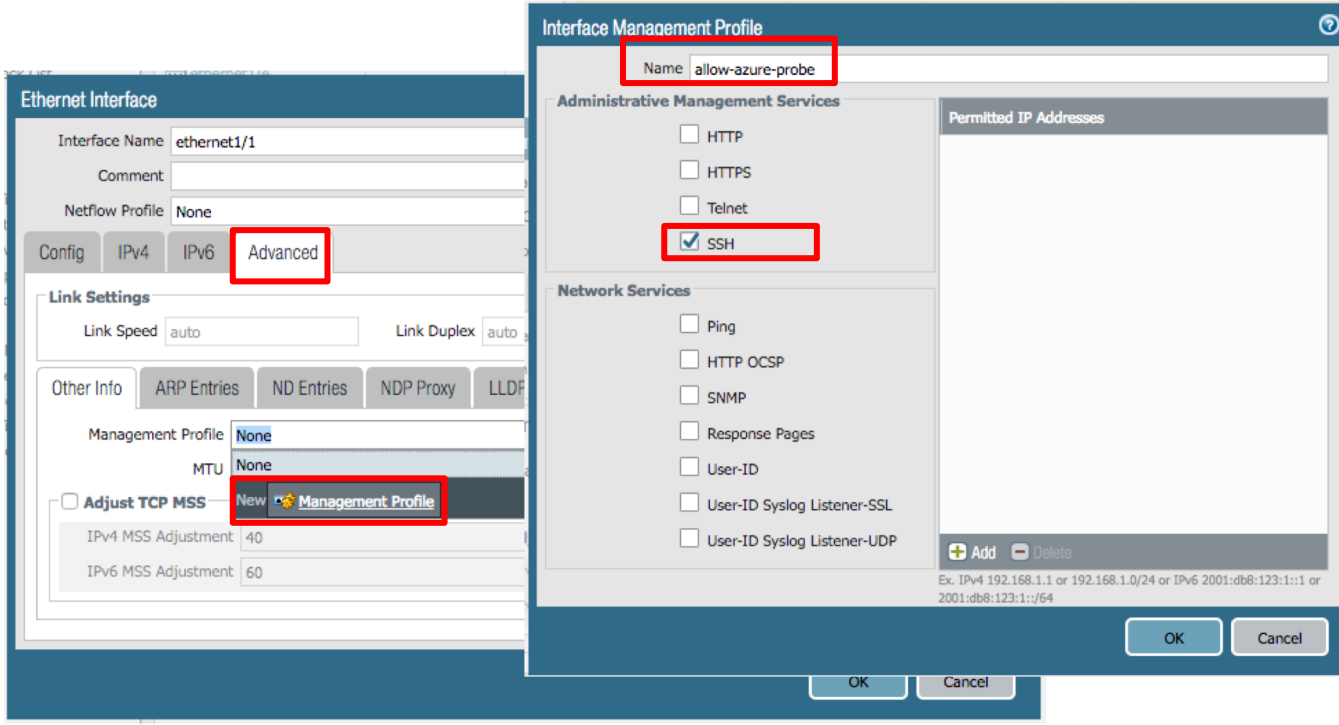
Step B5. Set Ethernet1/1 to DHCP

1. While still inside ethernet1/1, click IPv4 Tab.
2. Check DHCP Client (we will pull whatever IP Address Azure is giving us).
3. Uncheck “Automatically create default route pointing to default gateway provided by server.”

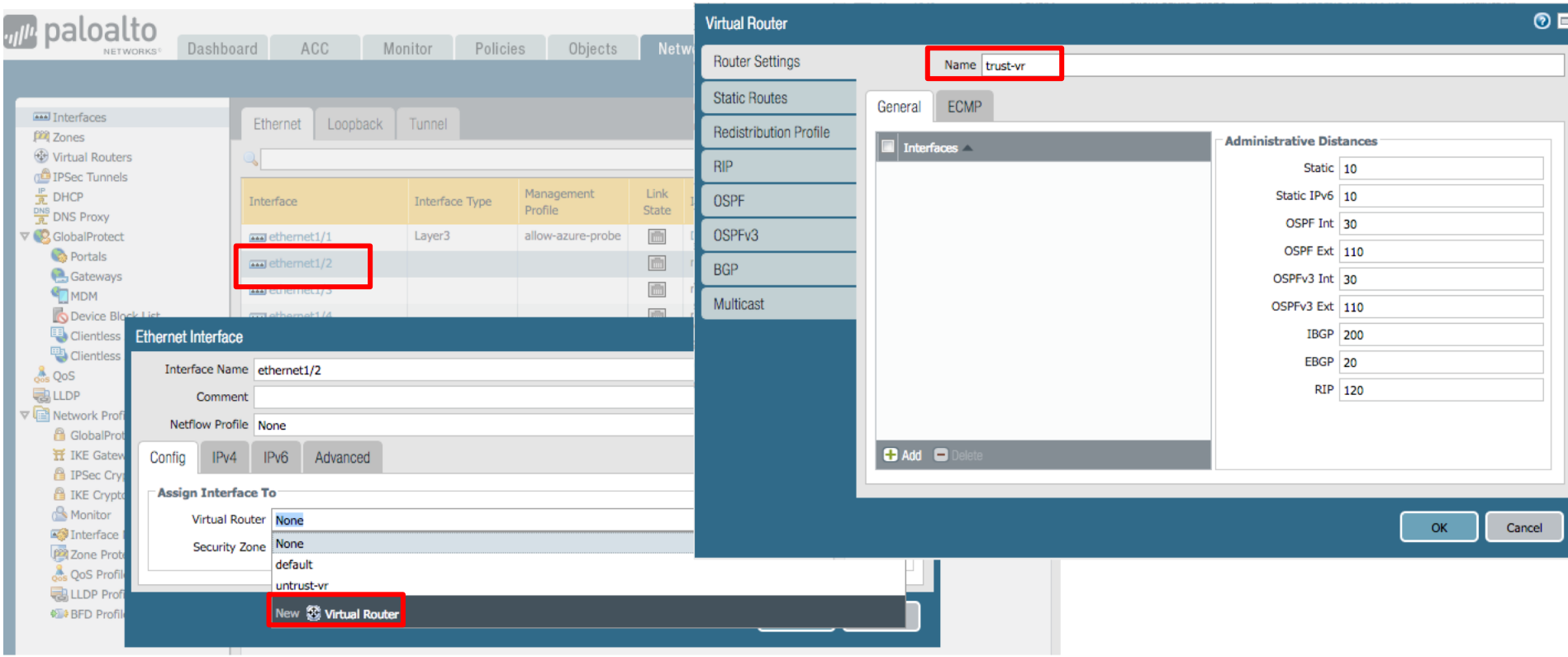


Step B6. Assign Management Profile to Ethernet1/1

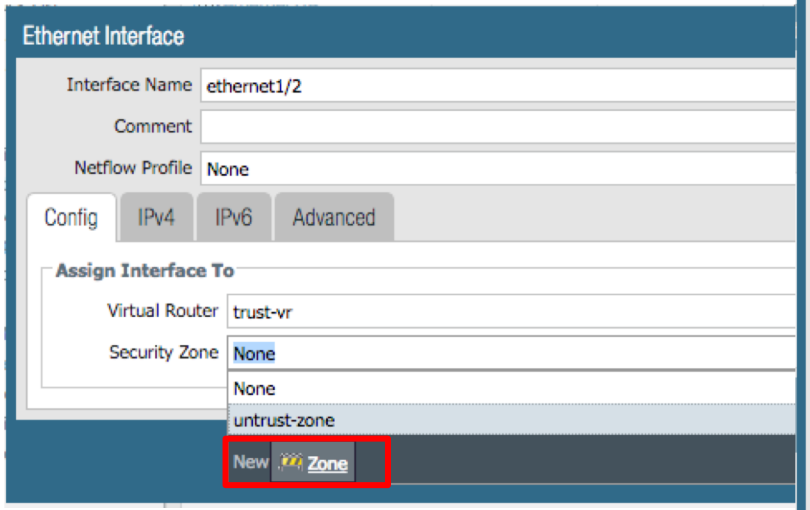
1. While still inside ethernet1/1, click Advanced Tab.
2. Click the Management Profile dropdown and select New Management Profile.
3. Enable SSH, click OK

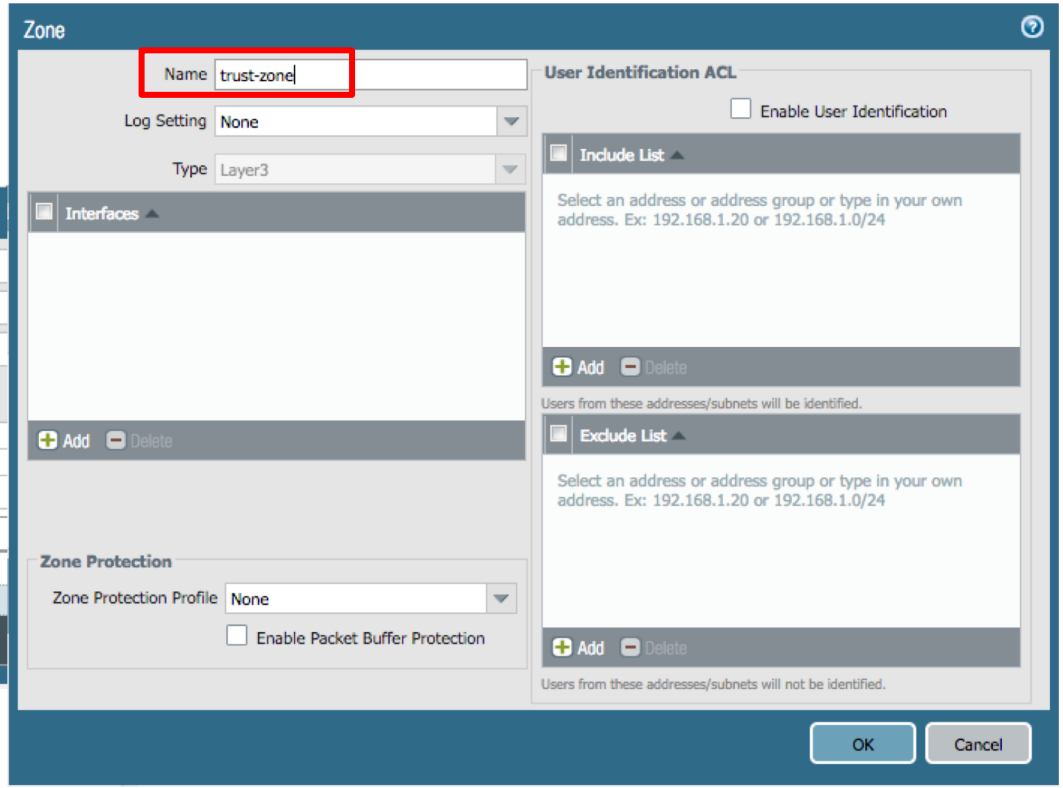


Step B7. Assign Virtual Router to Ethernet1/2

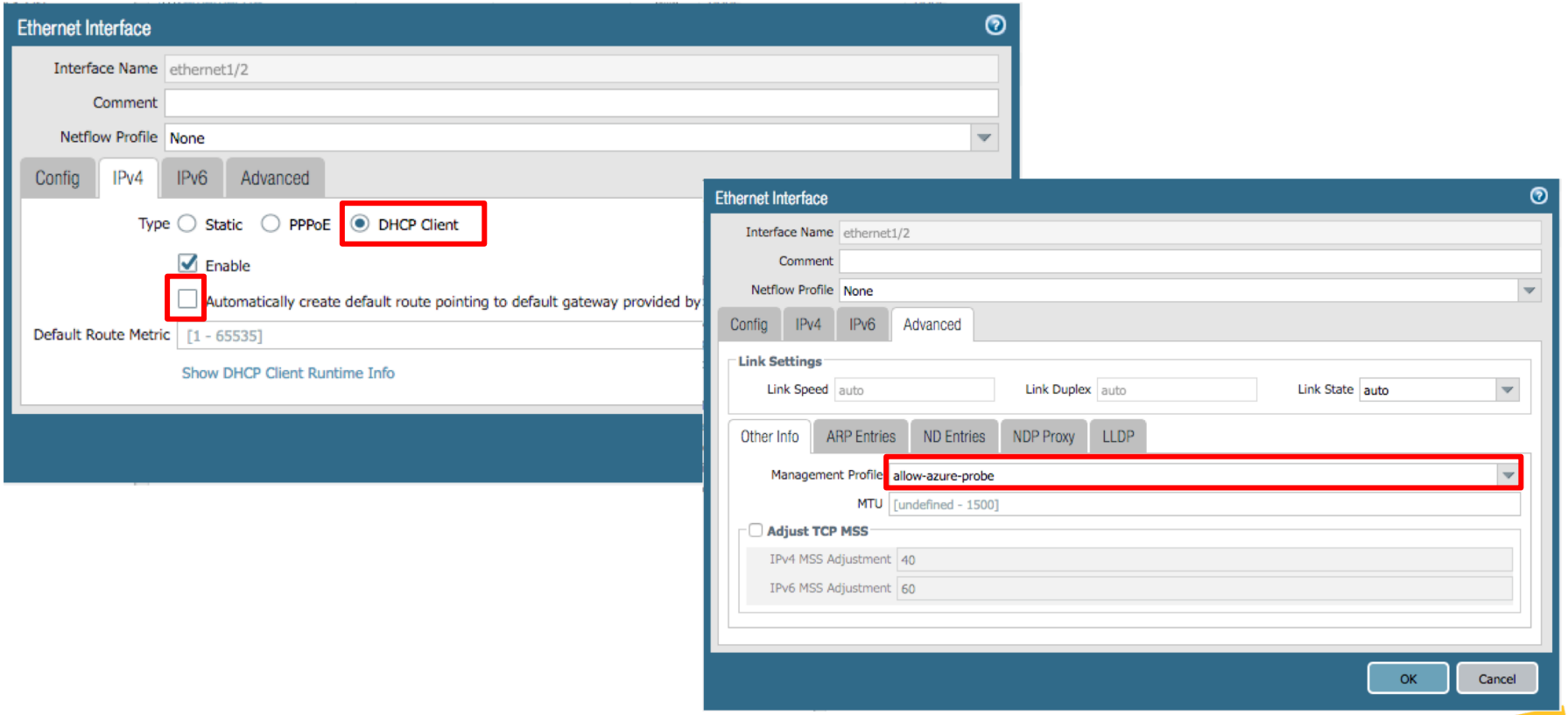


Step B8. Assign Zone to Ethernet1/2





Step B9. Find FW-1 Management IP.



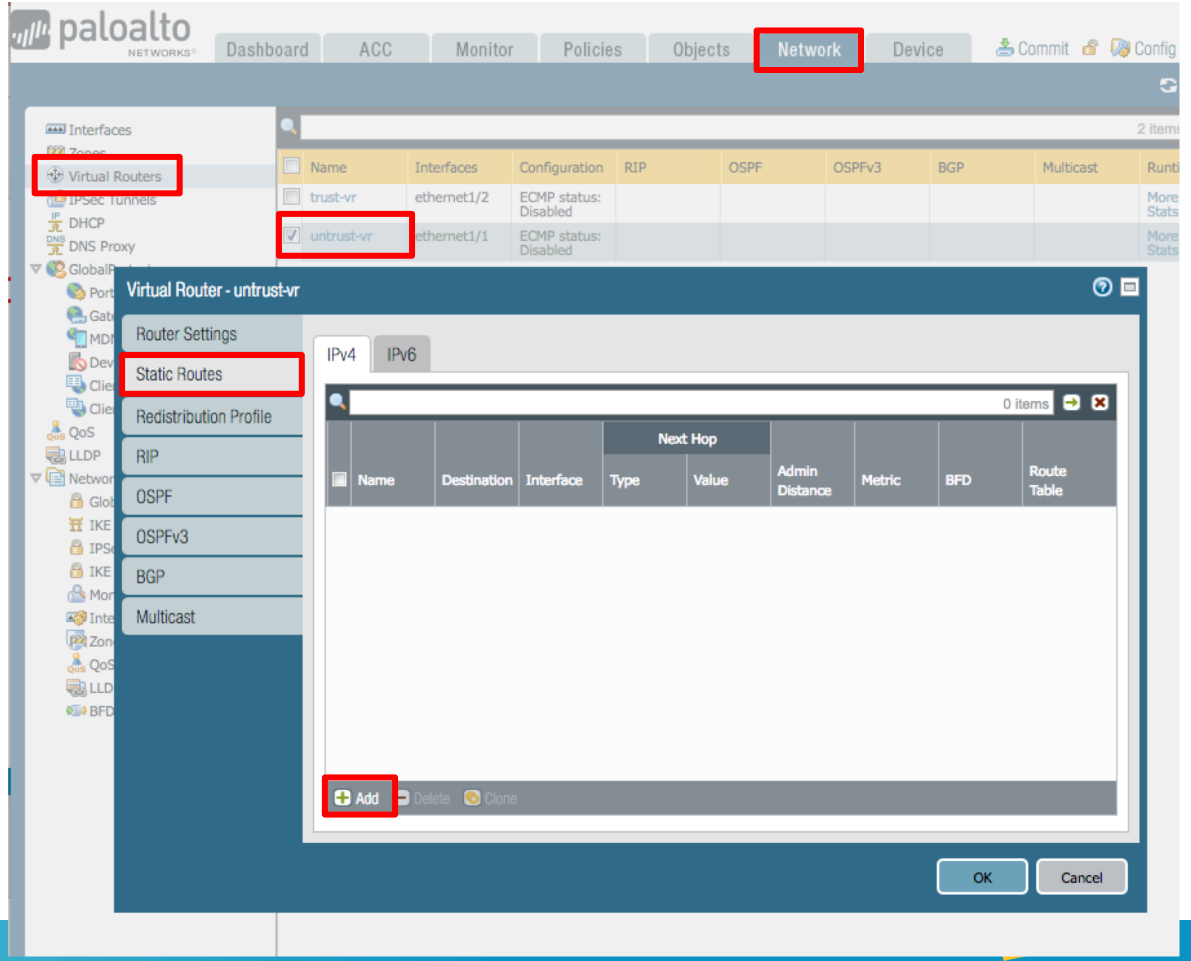
Repeat these steps on FW2 using the same settings.

Configure Routing on Virtual Routers

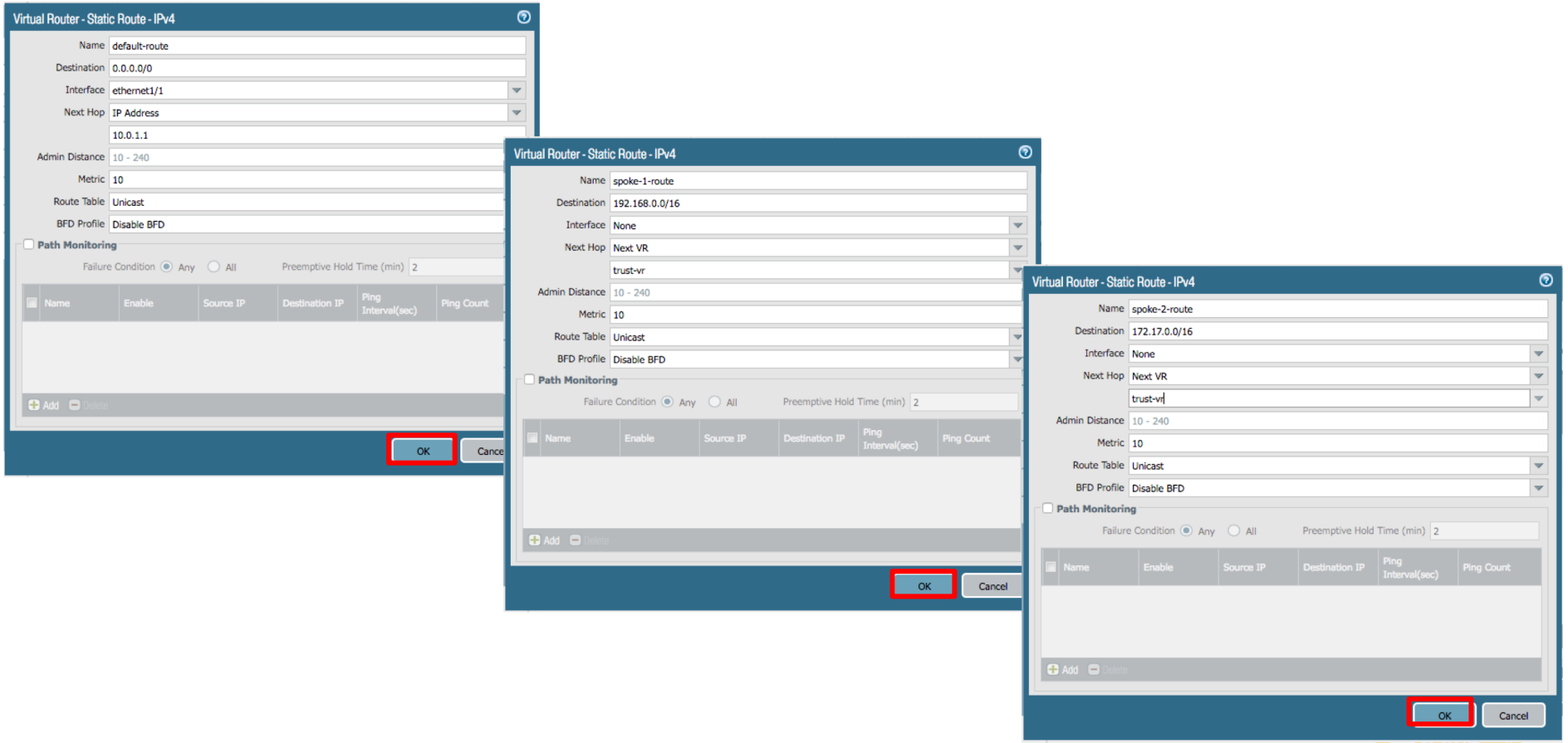
Step C1. Go to Untrust-VR

Go to:

Network →
Virtual Routers →
untrust-vr →
Static Routes → Add

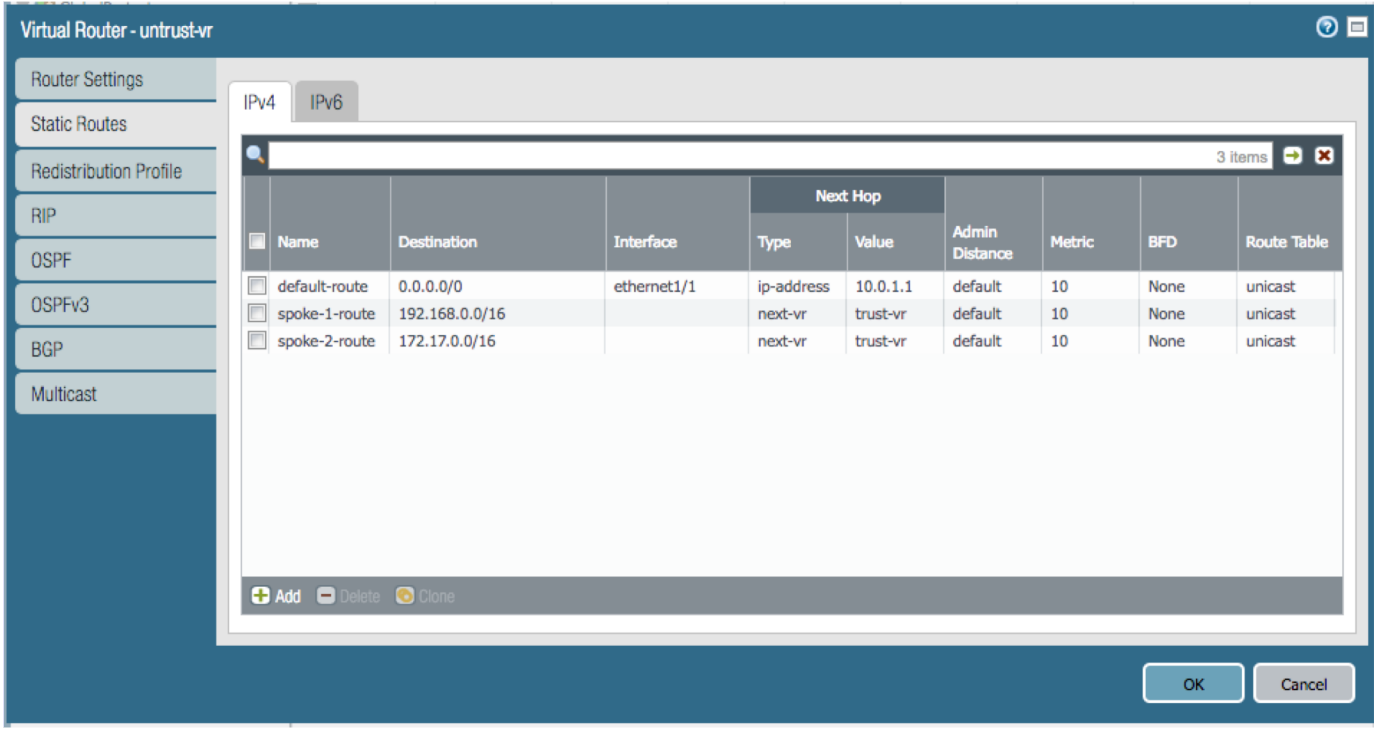


Step C2. Create 3 Routes in Untrust-VR



Untrust-VR Route Summary

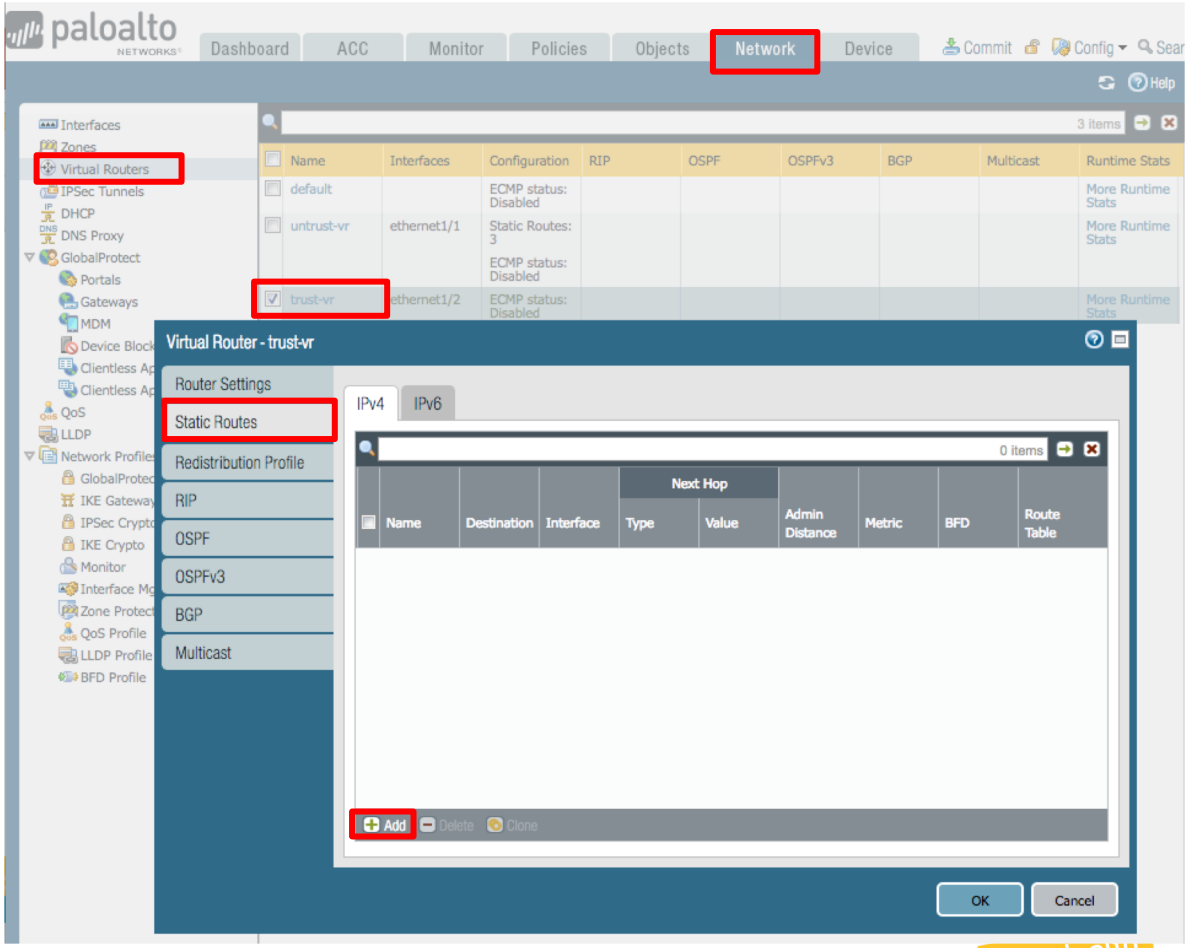
You should have 3 routes like the image to the left.



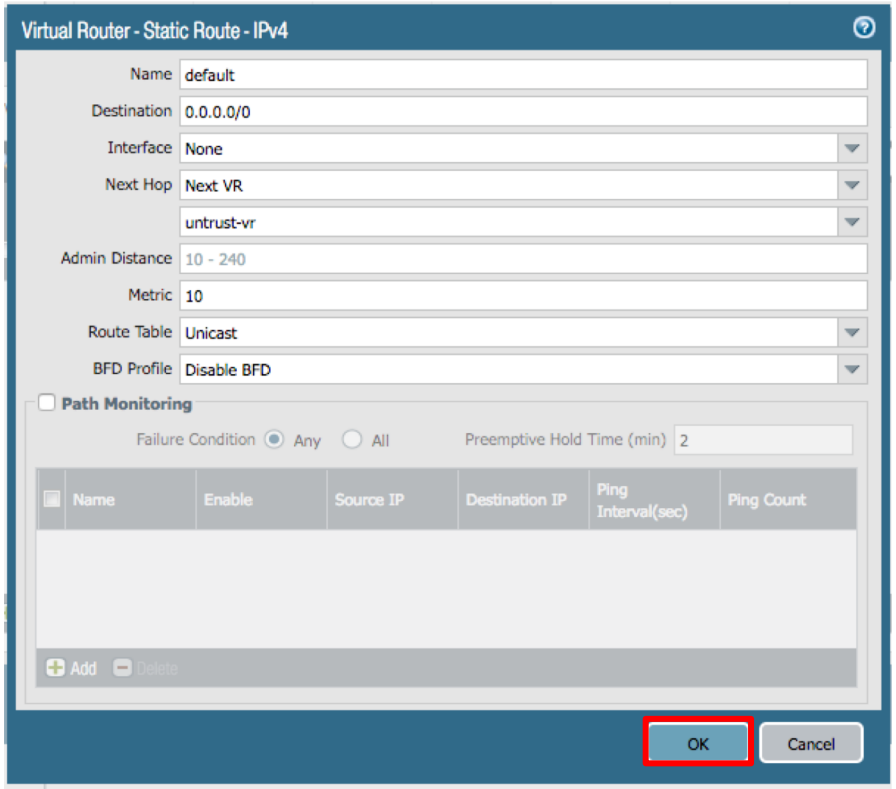
Step C3. Go to Trust-VR

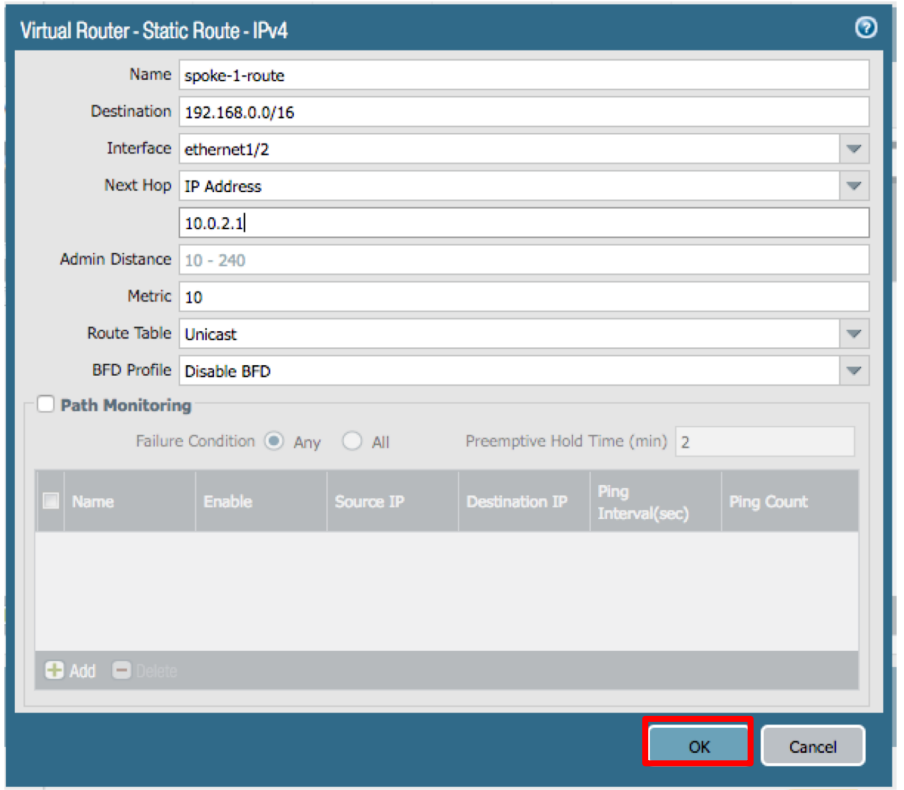
Go to:

Network →
Virtual Routers →
trust-vr →
Static Routes → Add

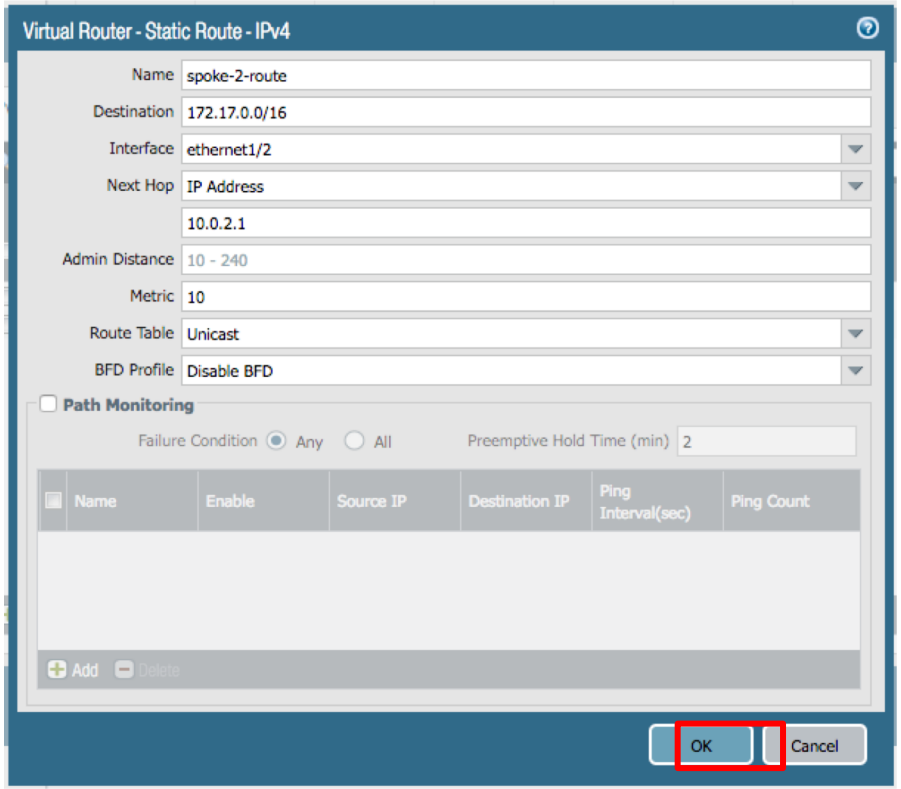


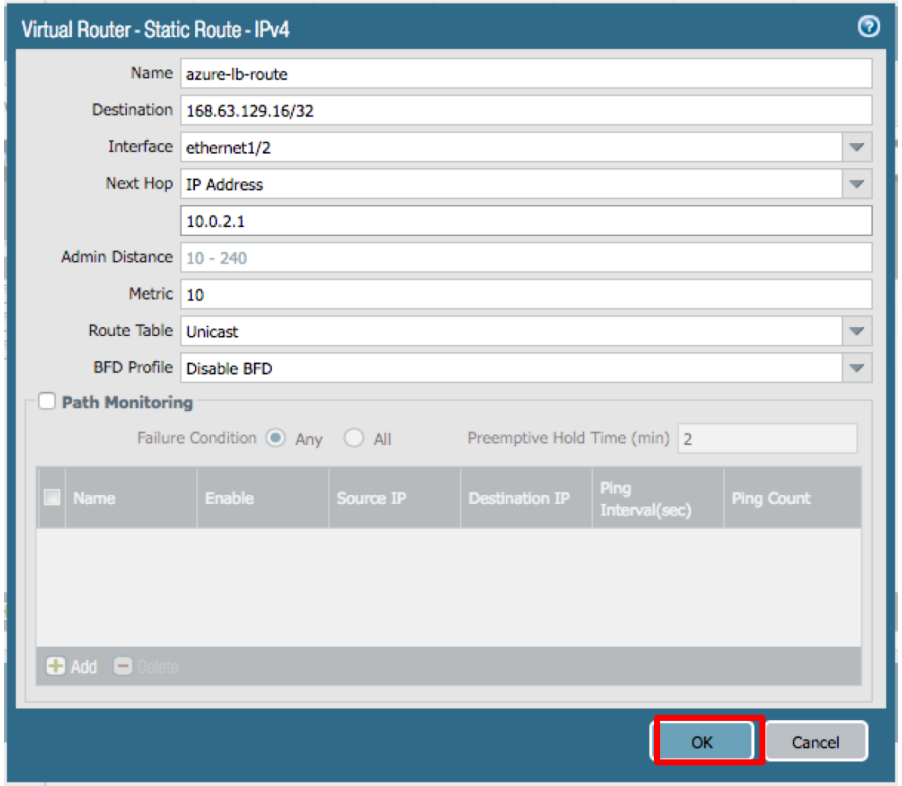
Step C4 (pt 1). Create Routes on Trust-VR





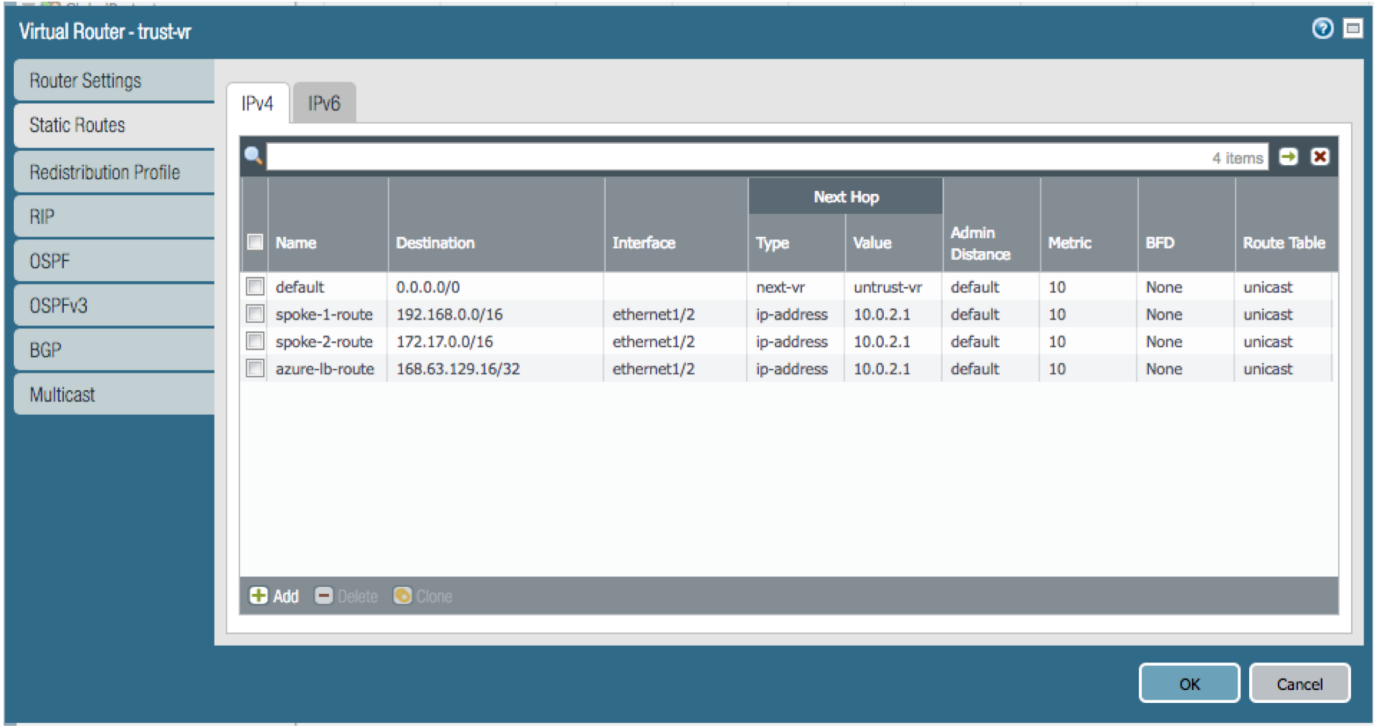
Step C4 (pt 2). Create Routes on Trust-VR





Trust-VR Route Summary

You should have 4 routes like the image to the left.



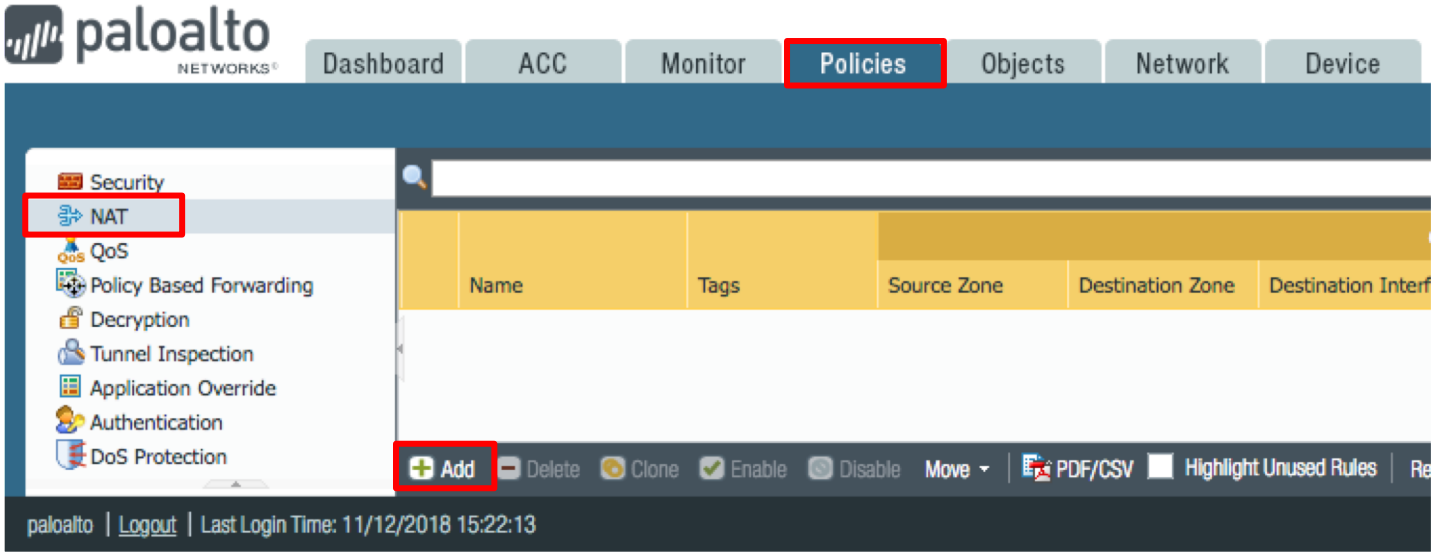
Repeat these steps on FW2 using the same exact routes.

Configure NAT Policies

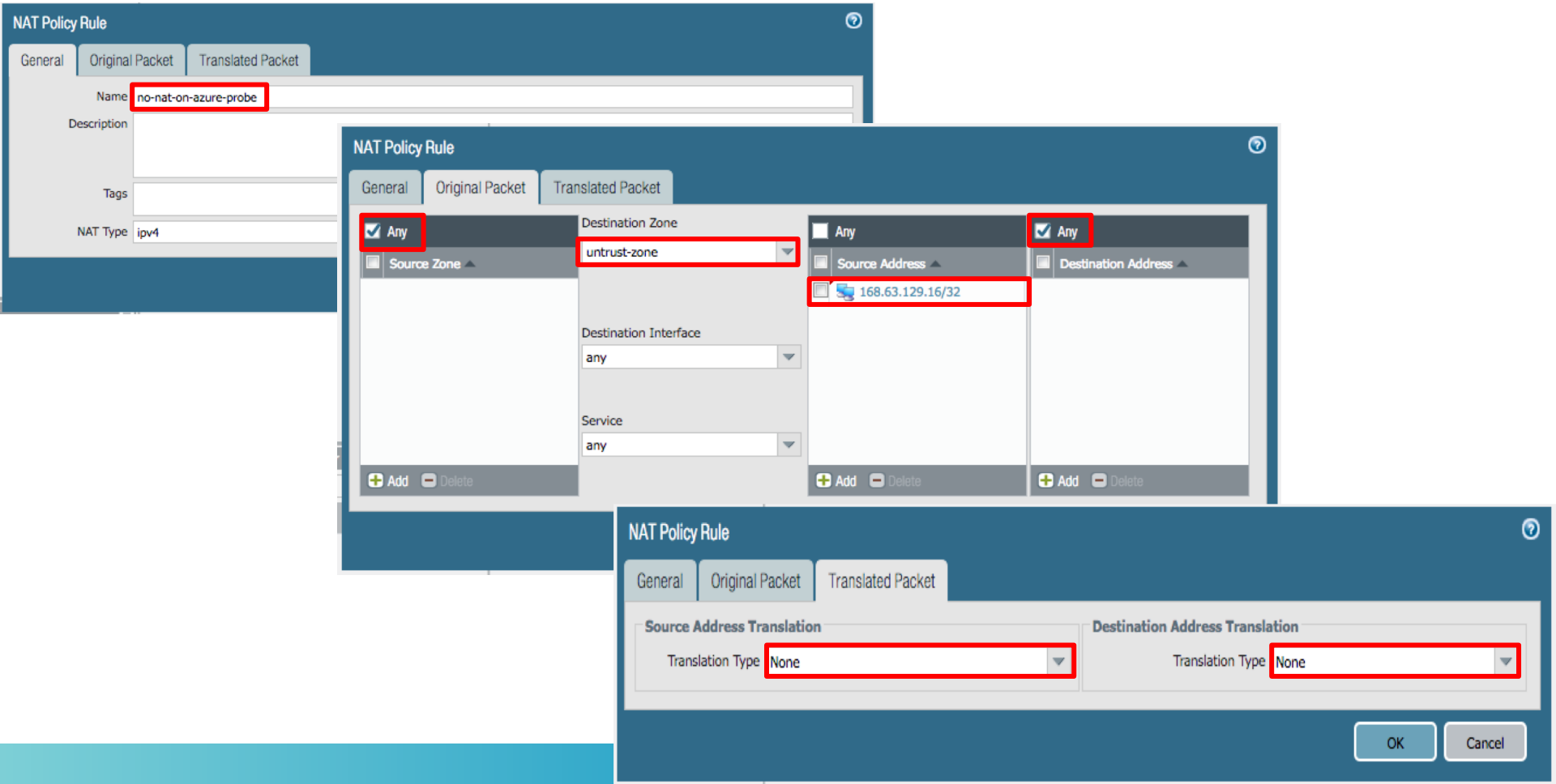
NAT Policy Overview

We need to create 4 NAT Policies.

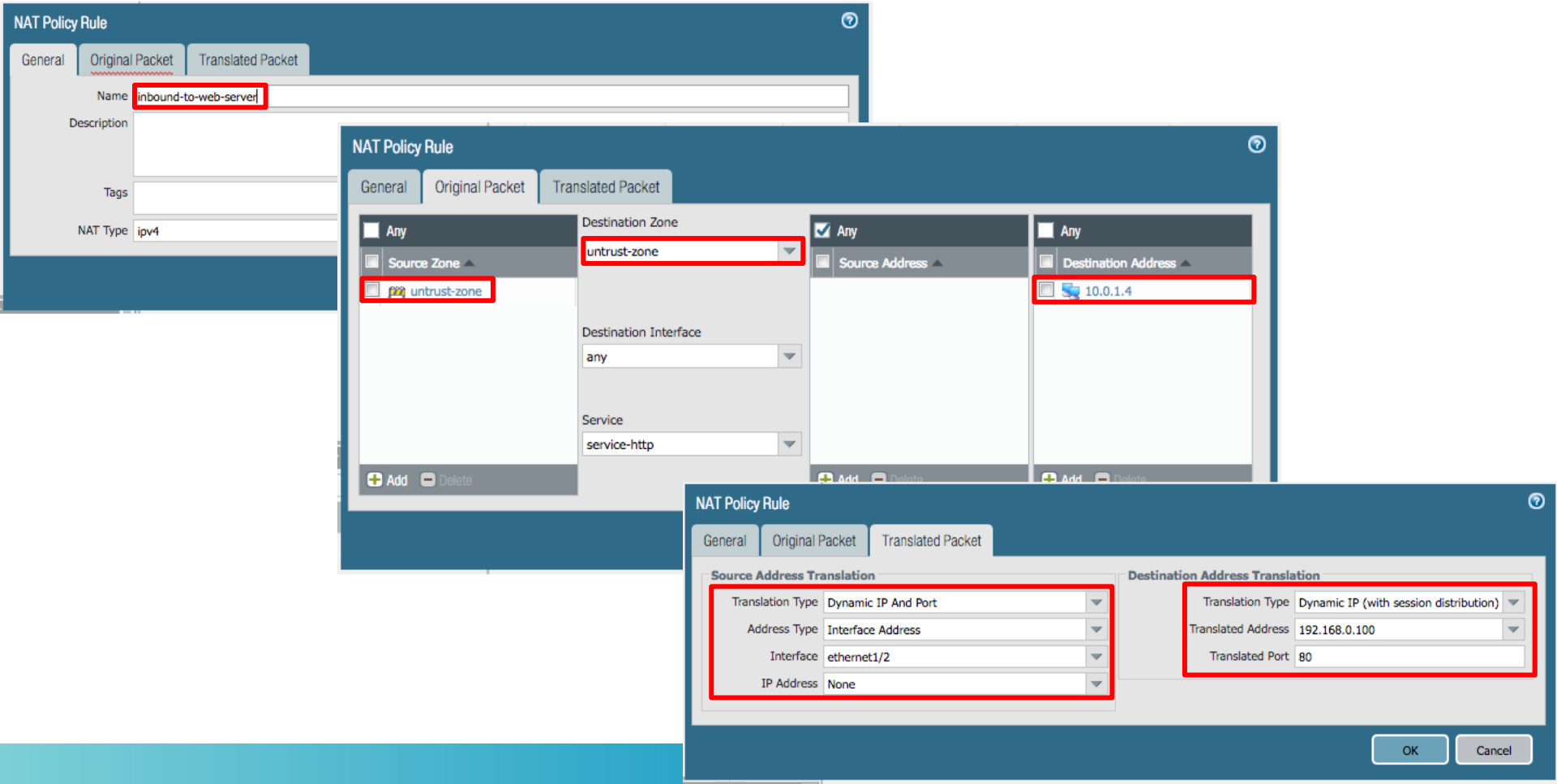
1. No-NAT on Azure Probe
2. DNAT to Web LB
3. DNAT to Jump VM
4. SNAT for Internet



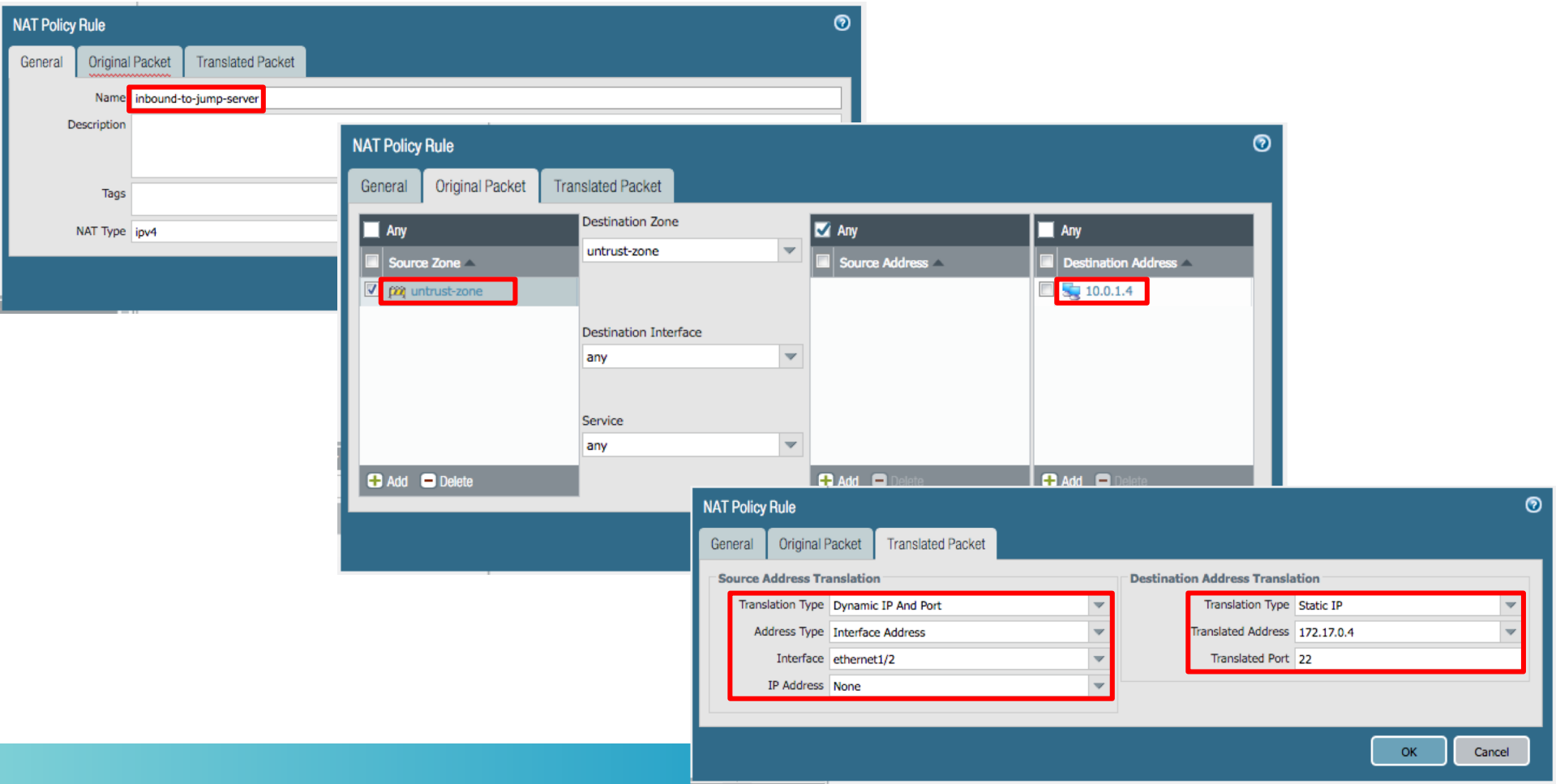
Step D1. Create No-NAT Policy for Azure Probe



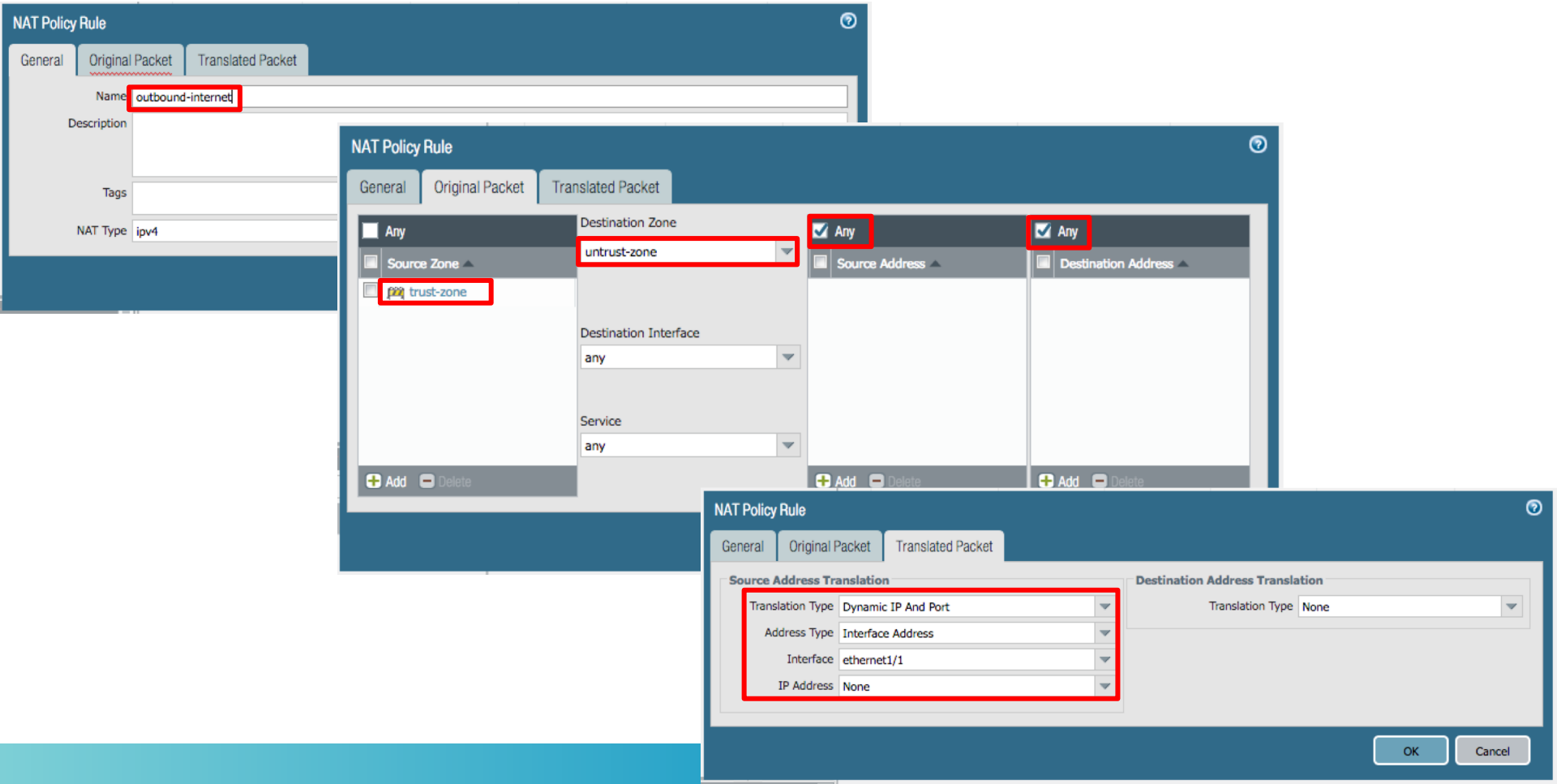
Step D2. Create DNAT Policy to Web-LB



Step D3. Create DNAT Policy to Jump VM



Step D4. Create SNAT Policy for Internet



NAT Policy Summary

Once completed, your 4 NAT policies should like the image below.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	no-nat-on-azure-probe	none	any	untrust-zone	any	168.63.129.16/...	any	any	none	none
2	inbound-to-web-server	none	untrust-zone	untrust-zone	any	any	10.0.1.4	service-http	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 192.168.0.100 port: 80
3	inbound-to-jump-ser...	none	untrust-zone	untrust-zone	any	any	10.0.1.4	any	dynamic-ip-and-port ethernet1/2	destination-translation address: 172.17.0.4 port: 22
4	outbound-internet	none	trust-zone	untrust-zone	any	any	any	any	dynamic-ip-and-port ethernet1/1	none

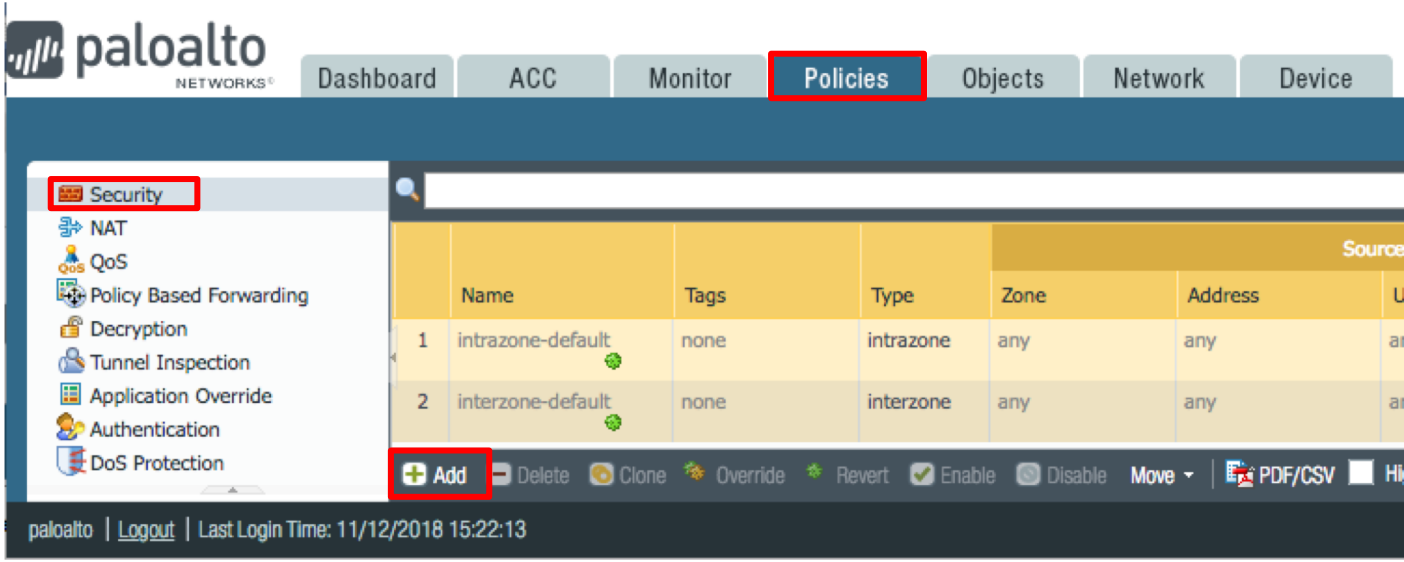
Repeat these steps for FW2, but set the destination address from 10.0.1.4 to 10.0.1.5 in your DNAT policies.

Configure Security Policies
&
Commit Changes

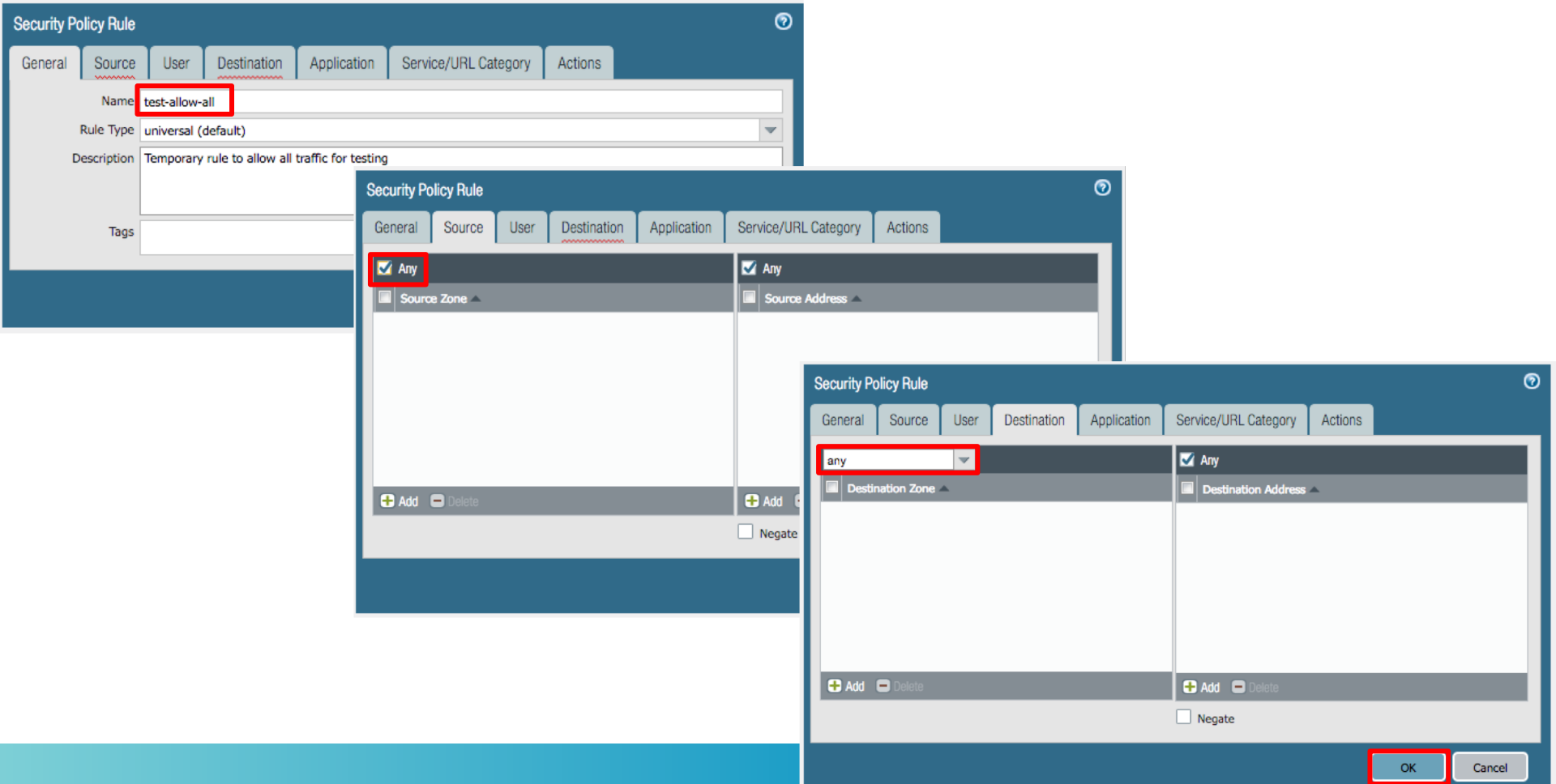
Step E1. Create a New Security Policy

We need to create 1 Security Policy to Allow-All Traffic.

THIS IS TEMPORARY FOR TESTING PURPOSES ONLY.



Step E2. Configure the Security Policy



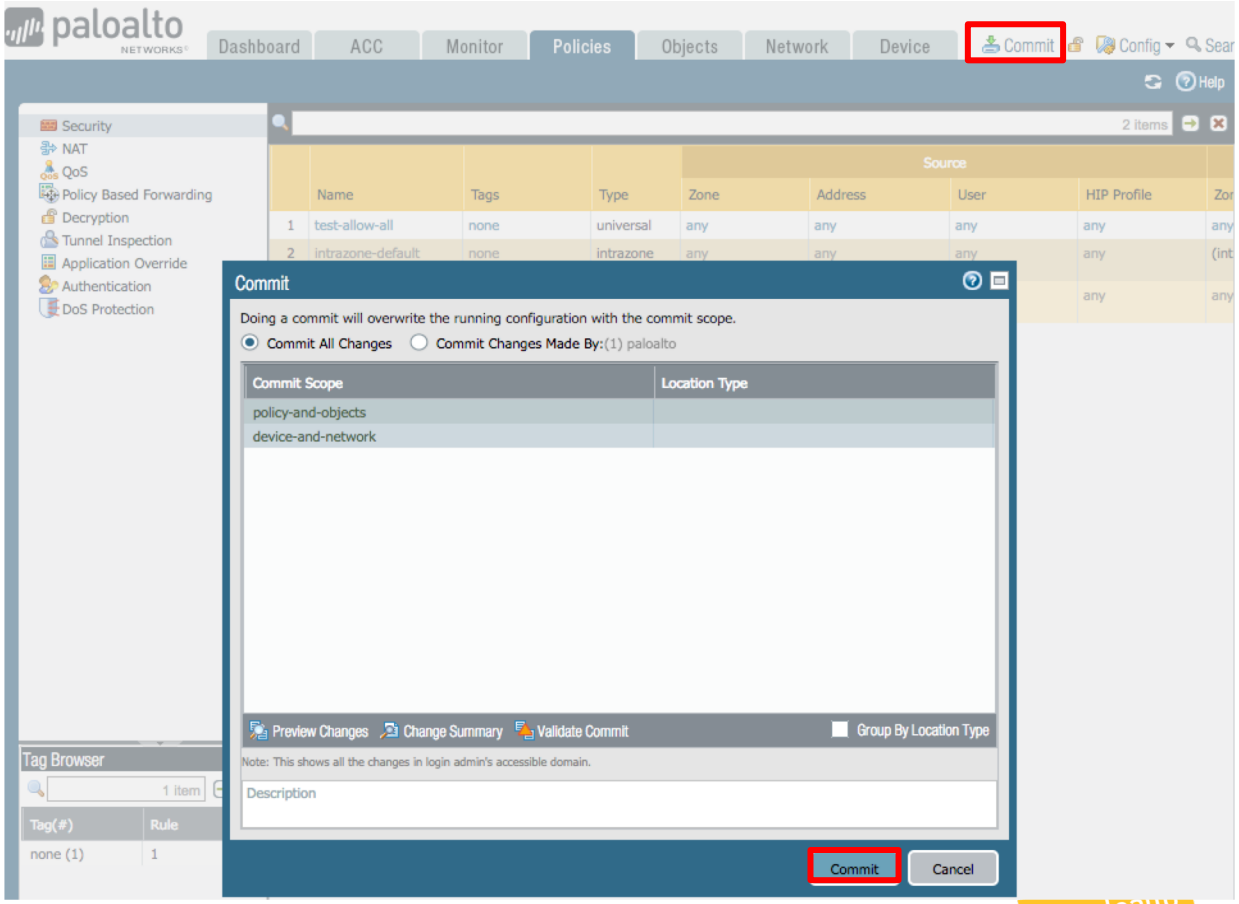
Security Policy Summary

Once completed, your test Security Policy should like the image below

				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	test-allow-all	none	universal	any	any	any	any	any	any	any	application-d...	Allow

Step E3. Commit all our Changes

Commit all the changes we made to the firewall by clicking Commit in the top right corner and selecting Commit again.

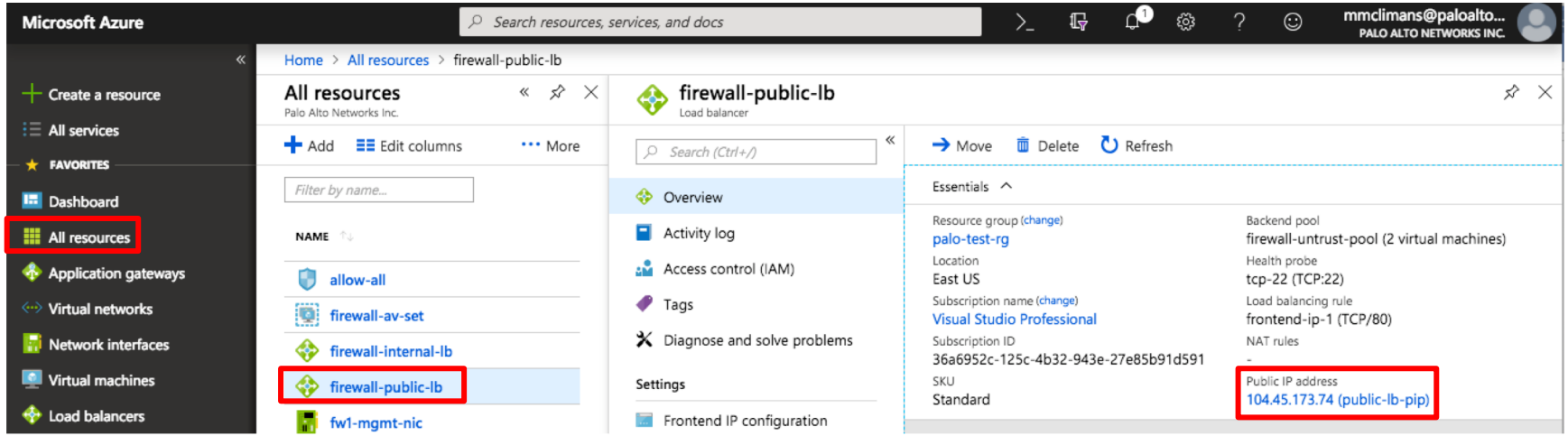


Repeat these steps for FW2.

Test the Deployment

Step F1. Find Public LB Public IP

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



Step F2. SSH into VM and test Traffic Flows.

Step 1. Open an SSH session using the hostname, username, and password below.

Hostname: Your-Public-LB-IP
Username: paloalto
Password: PanPassword123!

```
DFWMACW113G8WL:~ mmclimans$ ssh paloalto@104.45.173.74
```

Step 2. Try pinging out 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
```

Step 3. Try pinging to the other Spoke VNET

```
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
```

Step F3. SSH into Web VM and install Apache

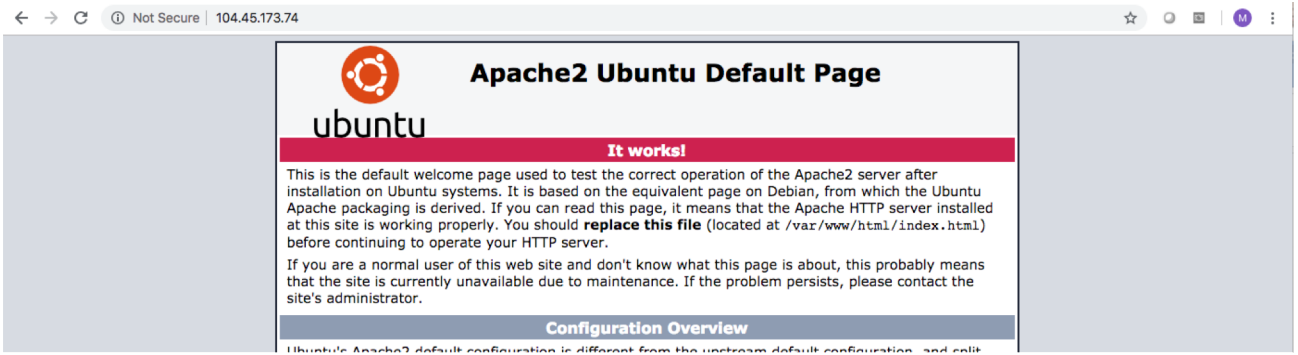
Step 1. While in the jump-vm, SSH to the Web-VM in Spoke-1-VNET

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

Step 2. Install apache by entering `sudo apt-get install apache2`

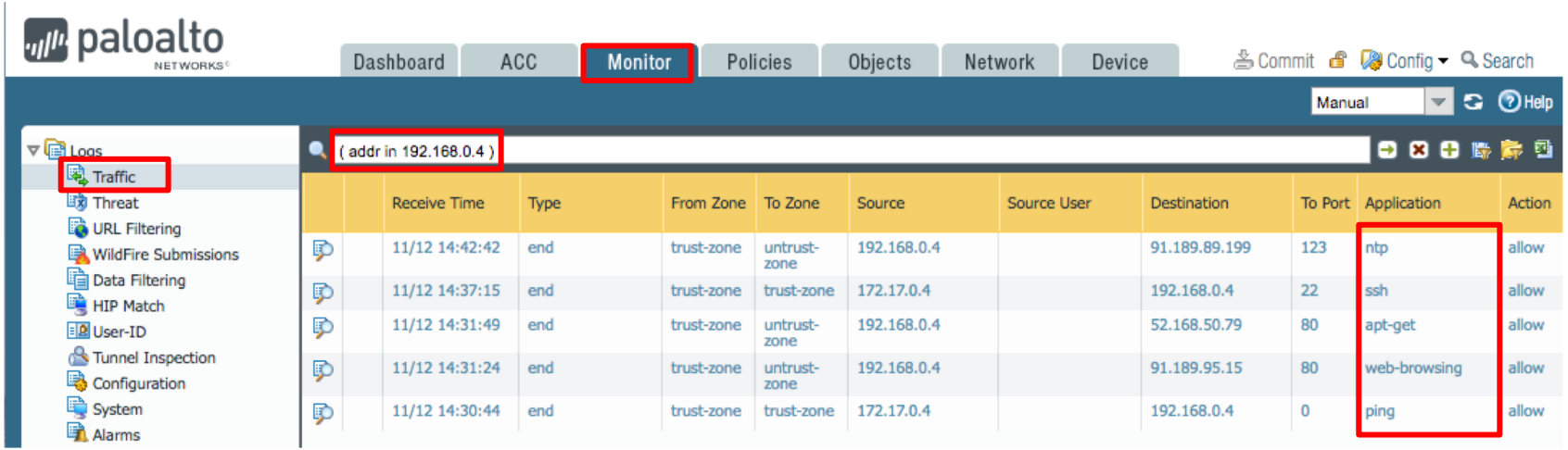
```
paloalto@web-vm:~$ sudo apt-get install apache2 -y
```

Step 3. Paste the Public Load Balancers IP into your browser (i.e. http://<your-ip-here>) and a Apache page should open.



Step F4. Filter Firewall Traffic Logs for your tested Traffic

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



If you do not see logs, check FW2.

Thank you!