

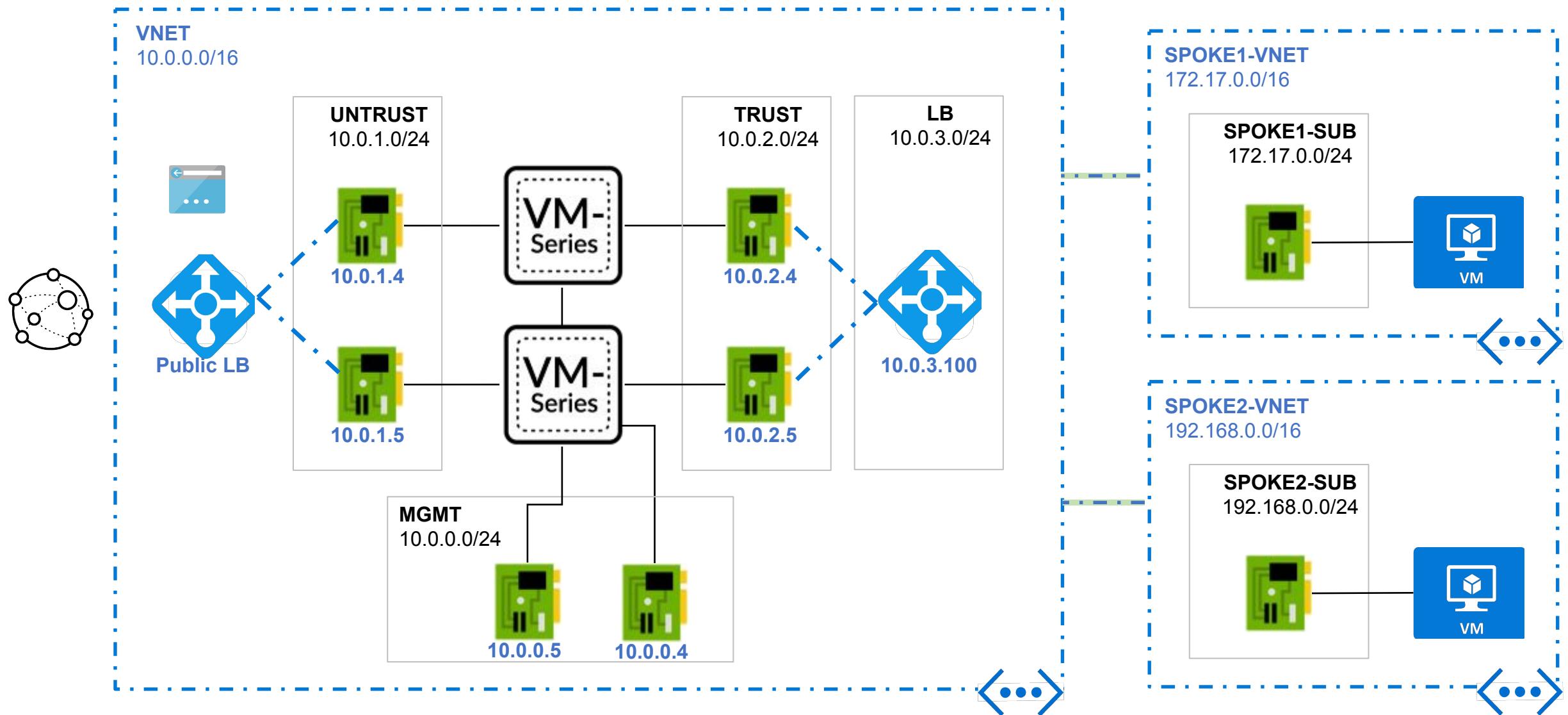


Prisma Public Cloud - Azure

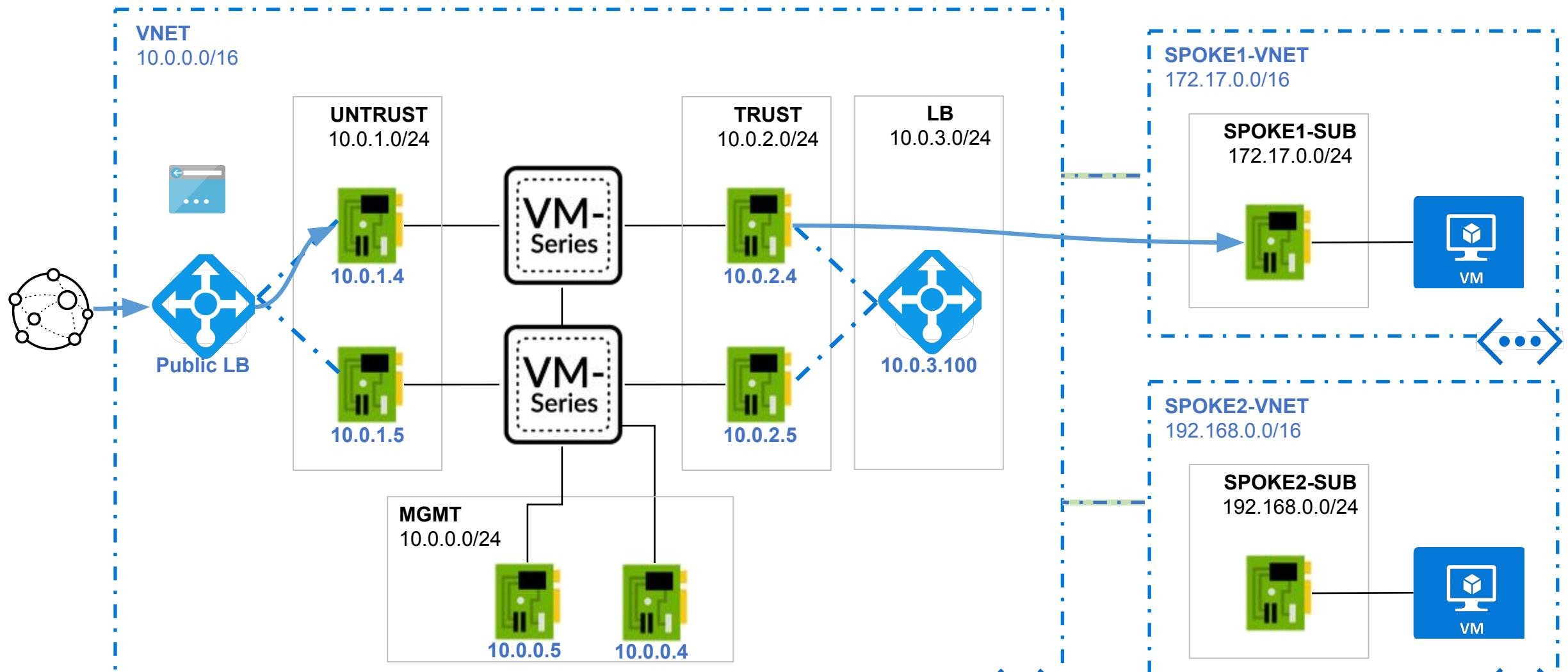
Lab Guide



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

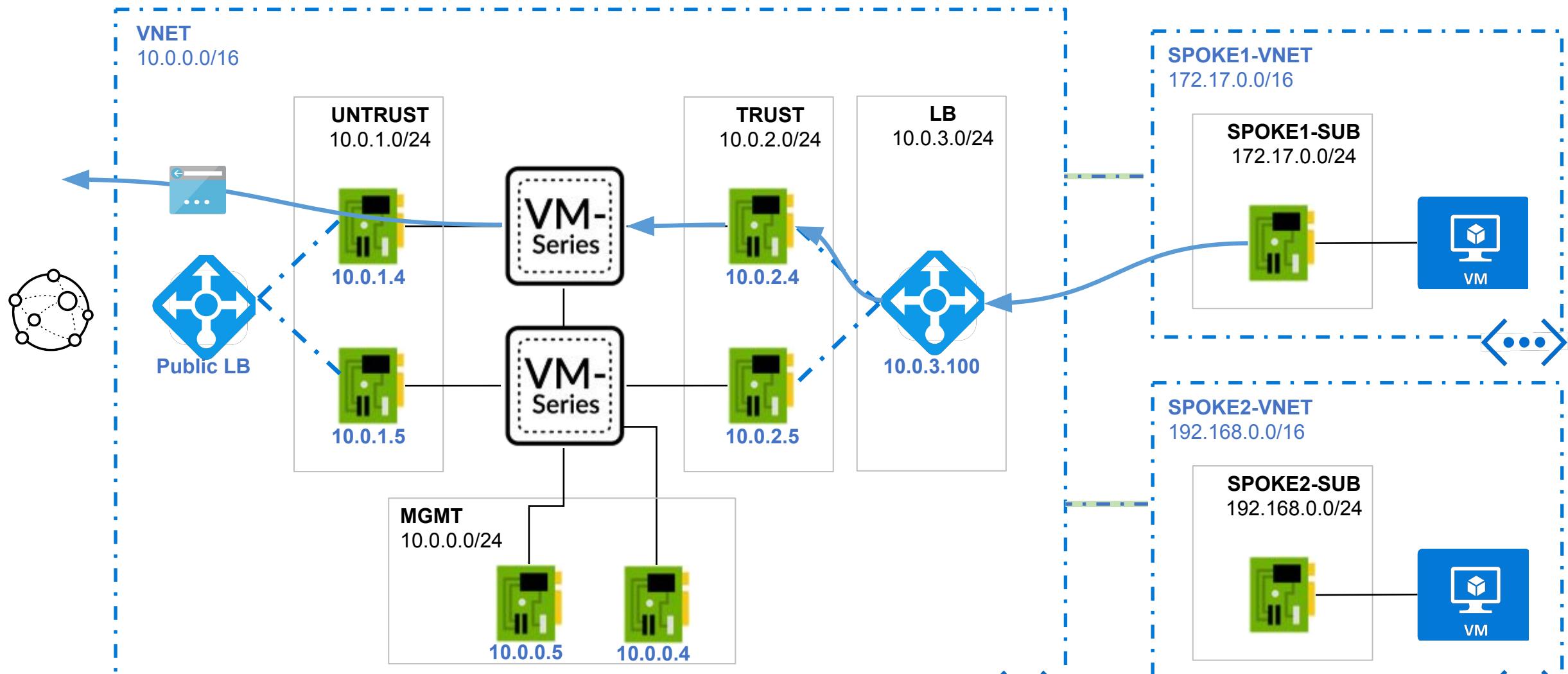


INBOUND TRAFFIC FLOW



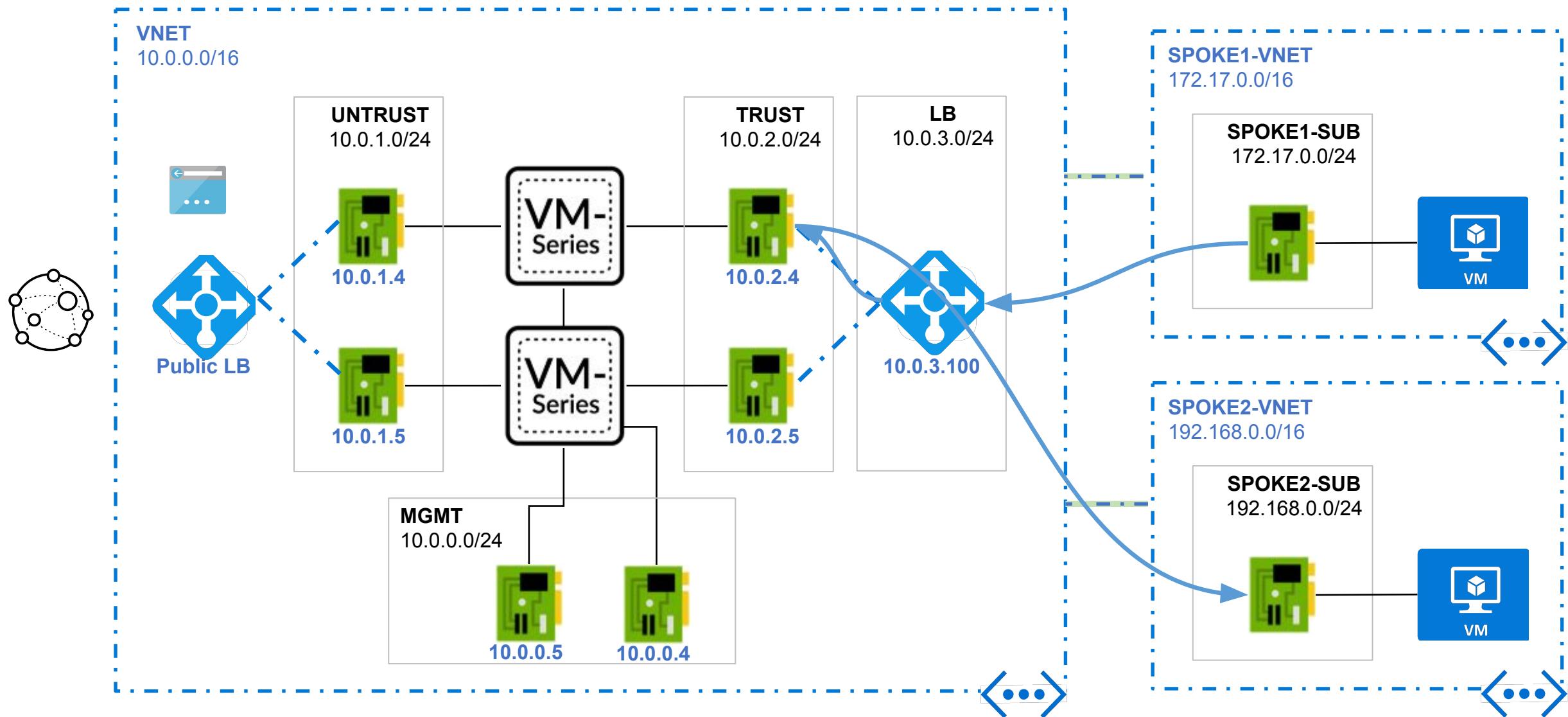
	Name	Tags	Original Packet							Translated Packet	
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service		Source Translation	Destination Translation
2	inbound-spoke1	none	untrust-zone	untrust-zone	any	any	untrust-nic	any		dynamic-ip-and-port	destination-translation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

OUTBOUND TRAFFIC FLOW CONFIGURATION



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

EAST-WEST TRAFFIC FLOW CONFIGURATION



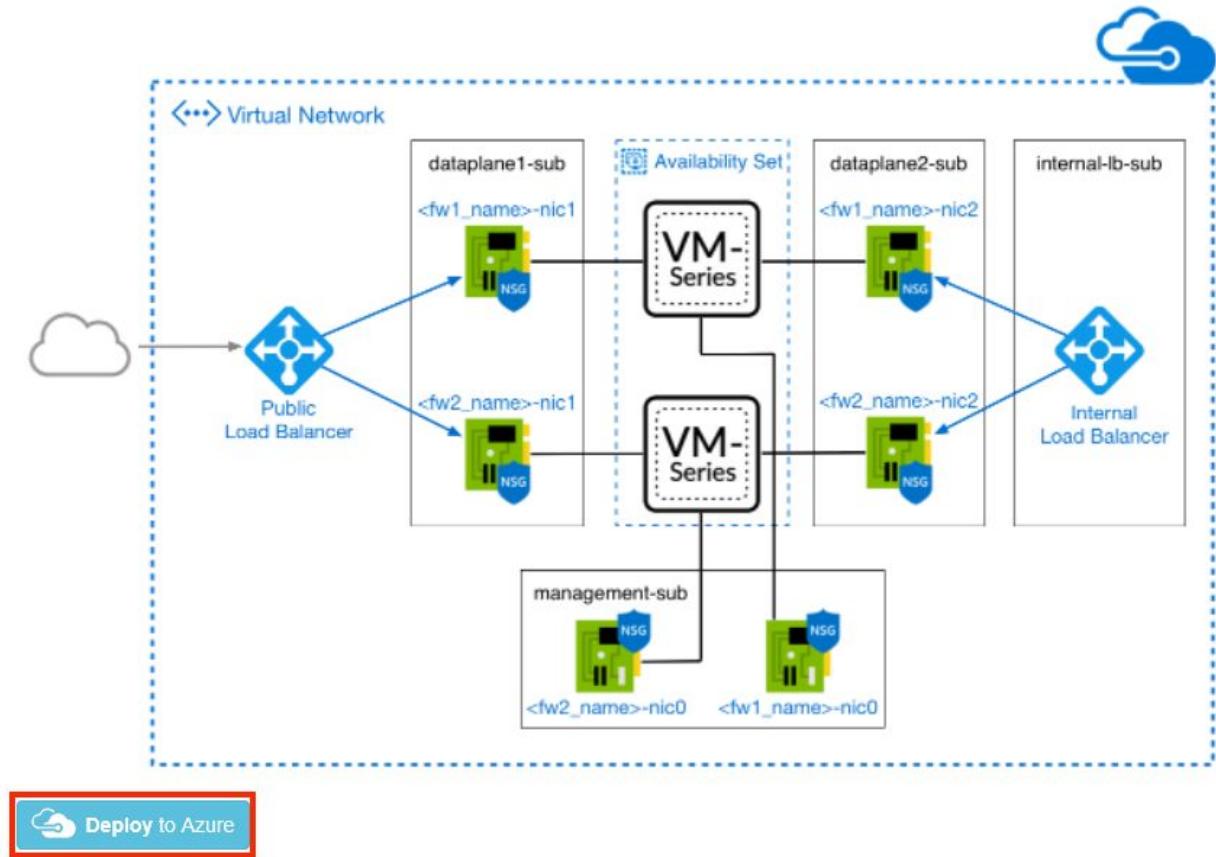
Deploy environment

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

Home >

Custom deployment

Deploy from a custom template

Template

 Customized template ↗
7 resources

 Edit template  Edit parameters  Visualize

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

AzureGCSPS ▼

Resource group * ⓘ

1 ▼
Create new

Instance details

Region * ⓘ

2 Norway East ▼

VNET Option ⓘ

3 Create new VNET ▼

VNET Resource Group ⓘ

4 ▼

VNET Name ⓘ

5 vmseries-vnet ▼

VNET Prefix ⓘ

6 10.0.0.0/16 ▼

Subnet Name-Management ⓘ

7 mgmt-subnet ▼

Subnet Name-Dataplane1 ⓘ

8 untrust-subnet ▼

Subnet Name-Dataplane2 ⓘ

9 trust-subnet ▼

Subnet Name-Internal LB ⓘ

10 lb-subnet ▼

Subnet Prefix-Management ⓘ

11 10.0.0.0/24 ▼

Subnet Prefix-Dataplane1 ⓘ

12 10.0.1.0/24 ▼

Subnet Prefix-Dataplane2 ⓘ

13 10.0.2.0/24 ▼

Subnet Prefix-Internal LB ⓘ

14 10.0.3.0/24 ▼

Public LB Name ⓘ

15 vmseries-public-lb ▼

Public LB Allowed Ports ⓘ

16 80, 443, 22, 3389 ▼

Internal LB Name ⓘ

17 vmseries-internal-lb ▼

Internal LB Address ⓘ

18 10.0.3.100 ▼

Health Probe Port ⓘ

19 80 ▼

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

FW1-Name ⓘ	1 <input type="text" value="vmseries-fw-vm1"/>
FW1-IP Management ⓘ	2 <input type="text" value="10.0.0.4"/>
FW1-IP Dataplane1 ⓘ	3 <input type="text" value="10.0.1.4"/>
FW1-IP Dataplane2 ⓘ	4 <input type="text" value="10.0.2.4"/>
FW2-Name ⓘ	5 <input type="text" value="vmseries-fw-vm2"/>
FW2-IP Management ⓘ	6 <input type="text" value="10.0.0.5"/>
FW2-IP Dataplane1 ⓘ	7 <input type="text" value="10.0.1.5"/>
FW2-IP Dataplane2 ⓘ	8 <input type="text" value="10.0.2.5"/>
License Type ⓘ	9 <input type="text" value="byol"/> ▾
PANOS Version ⓘ	10 <input type="text" value="10.0.6"/> ▾
VM Size ⓘ	11 <input type="text" value="Standard_DS3_v2"/> ▾
OS Disk Type ⓘ	12 <input type="text" value="Standard_LRS"/> ▾
Availability Set Option ⓘ	13 <input type="text" value="Create new availability set"/> ▾
Availability Set Name ⓘ	14 <input type="text" value="vmseries-fw-as"/>
Accelerated Networking ⓘ	15 <input type="text" value="disable"/> ▾
Apply Public IP To Management ⓘ	16 <input type="text" value="Yes"/> ▾
Apply Public IP To Dataplane1 ⓘ	17 <input type="text" value="Yes"/> ▾
NSG Name ⓘ	18 <input type="text" value="vmseries-nsg"/>
NSG Source Prefix ⓘ	19 <input type="text" value="0.0.0.0/0"/>
Username ⓘ	20 <input type="text" value="paloalto"/>
Password * ⓘ	21 <input type="password"/> ⓘ
Optional-Bootstrap Storage Account ⓘ	<input type="text"/>
Optional-Bootstrap Access Key ⓘ	<input type="text"/> ⓘ
Optional-Bootstrap File Share Name ⓘ	<input type="text"/>
Optional-Bootstrap Share Directory ⓘ	<input type="text"/>
Optional-Append String To Resources ⓘ	<input type="text"/>

Review + create

< Previous

Next : Review + create >

Deploy Environment

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

Review + create

< Previous

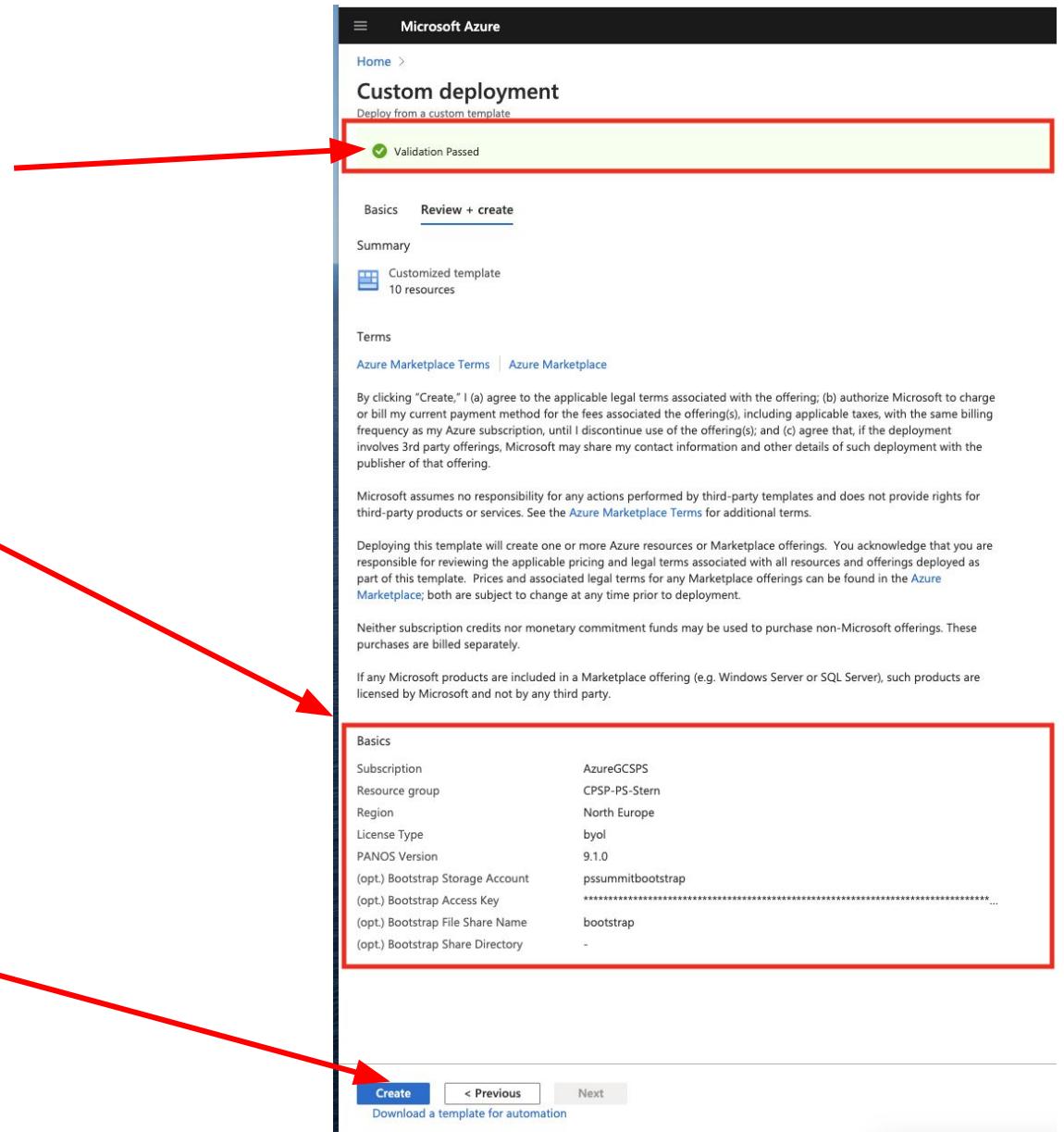
Next : Review + create >

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!

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "Microsoft.Template-20201118105252". The main message is "Your deployment is complete". Key details listed include:

- Deployment name: Microsoft.Template-20201118105252
- Subscription: AzureGCSPS
- Resource group: CPSP-PS-Stern

Below the summary, there are sections for "Deployment details" (with a download link) and "Next steps". A prominent blue button at the bottom center says "Go to resource group".

Deploy WebApp Resource Group

Deploy WebApp

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

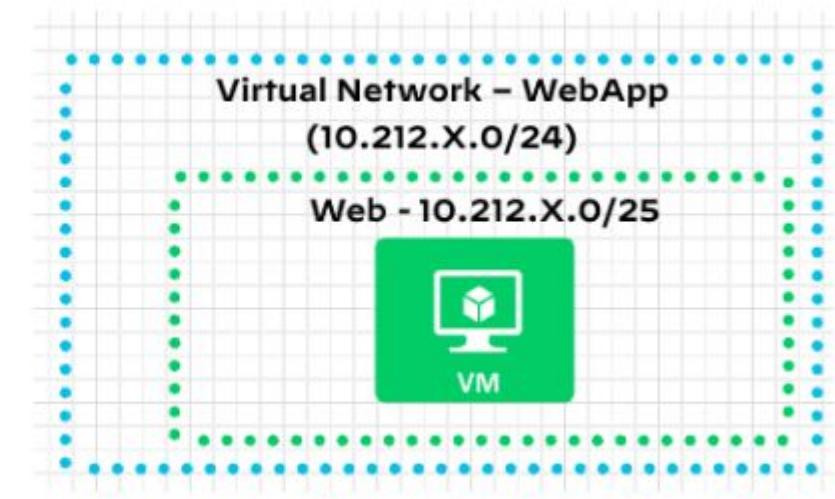
<https://github.com/PaloAltoNetworks/lab-azure-vmseries>

2. Click on “Deploy to Azure”

Part 2: Deploy WebApp (Basic/Advanced Lab)

In this part, We will Deploy a single Linux Server in a dedicated Resource Group

 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

Home >

Custom deployment

Deploy from a custom template

Basics Review + create

Template

Customized template  5 resources

 Edit template

 Edit parameters

Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * 

AzureGCSPS 

Resource group * 

(New) PSSummit-Instructor-Spoke 

Create new

Parameters

Region * 

North Europe 

Admin Username * 

fwadmin 

Admin Password * 

***** 

VNET Option 

Create new VNET 

VNET Resource Group 



Vm Name 

Web-App 

Virtual Network Name 

spoke-vnet 

Address Prefix 

10.212.1.0/24 

Subnet Name 

spoke-vnet-subnet 

Subnet Prefix 

10.212.1.0/25 

Review + create

< Previous

Next : Review + create >

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!

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "Microsoft.Template-20210201105503". The deployment status is shown as "Your deployment is complete" with a green checkmark icon. A red box highlights this message. Below it, deployment details are listed: Deployment name: Microsoft.Template-20210201105503, Subscription: AzureGCSPS, Resource group: pssummit-instructor-app. To the right, deployment metadata is provided: Start time: 2/1/2021, 10:55:04 AM and Correlation ID: c0426197-4bdf-40b6-8fd3-27c9a0da6fa5. At the bottom, there are sections for "Deployment details" and "Next steps". A red arrow points from the text "See below" in the previous slide to the "Go to resource group" button, which is highlighted with a red box.

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. Below the navigation bar, the breadcrumb trail shows 'Home > Microsoft.Template-20210201105503 >'. The main title is 'pssummit-instructor-app' under the 'Resource group' section. On the left, there is a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Events, Settings, Deployments, Security, Policies, Properties, Locks, Cost Management, and Cost analysis. The 'Overview' link is currently selected. The main content area displays the 'Essentials' section with details about the subscription (AzureGCSPS), deployment status (1 Succeeded), location (North Europe), and tags. Below this, there is a filter bar and a table listing 6 records. The table columns include Name, Type, and Location. The items listed are:

Name	Type	Location
simple-vm-instructor_disk1_9855dfa5bb1b4858bf15a24e2985579c	Disk	North Europe
myVMNic	Network interface	North Europe
default-NSG	Network security group	North Europe
bootdiagsniqu6mh22de	Storage account	North Europe
simple-vm-instructor	Virtual machine	North Europe
spoke-vnet-instructor	Virtual network	North Europe

Create VNET peering

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

Microsoft Azure

Search resources, services

Home > Microsoft Template-20210201105503 > pssummit-instructor-app > spoke-vnet-instructor

Show portal menu

spoke-vnet-instructor | Peerings

Virtual network

Search (Cmd+/) 2 Add Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Filter by name...

Name	Peering status
Add a peering to get started	

Settings

Address space Connected devices Subnets DDoS protection Firewall Security DNS servers

Peerings

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

Microsoft Azure

Home > Microsoft.Template-20210201105503 > pssummit-instructor-app > spoke-vnet-instructor >

Add peering

spoke-vnet-instructor

This virtual network

Peering link name * ✓

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ
 Use this virtual network's gateway
 Use the remote virtual network's gateway
 None (default)

Remote virtual network

Peering link name * ✓

Virtual network deployment model ⓘ
 Resource manager
 Classic

I know my resource ID ⓘ

Subscription * ⓘ

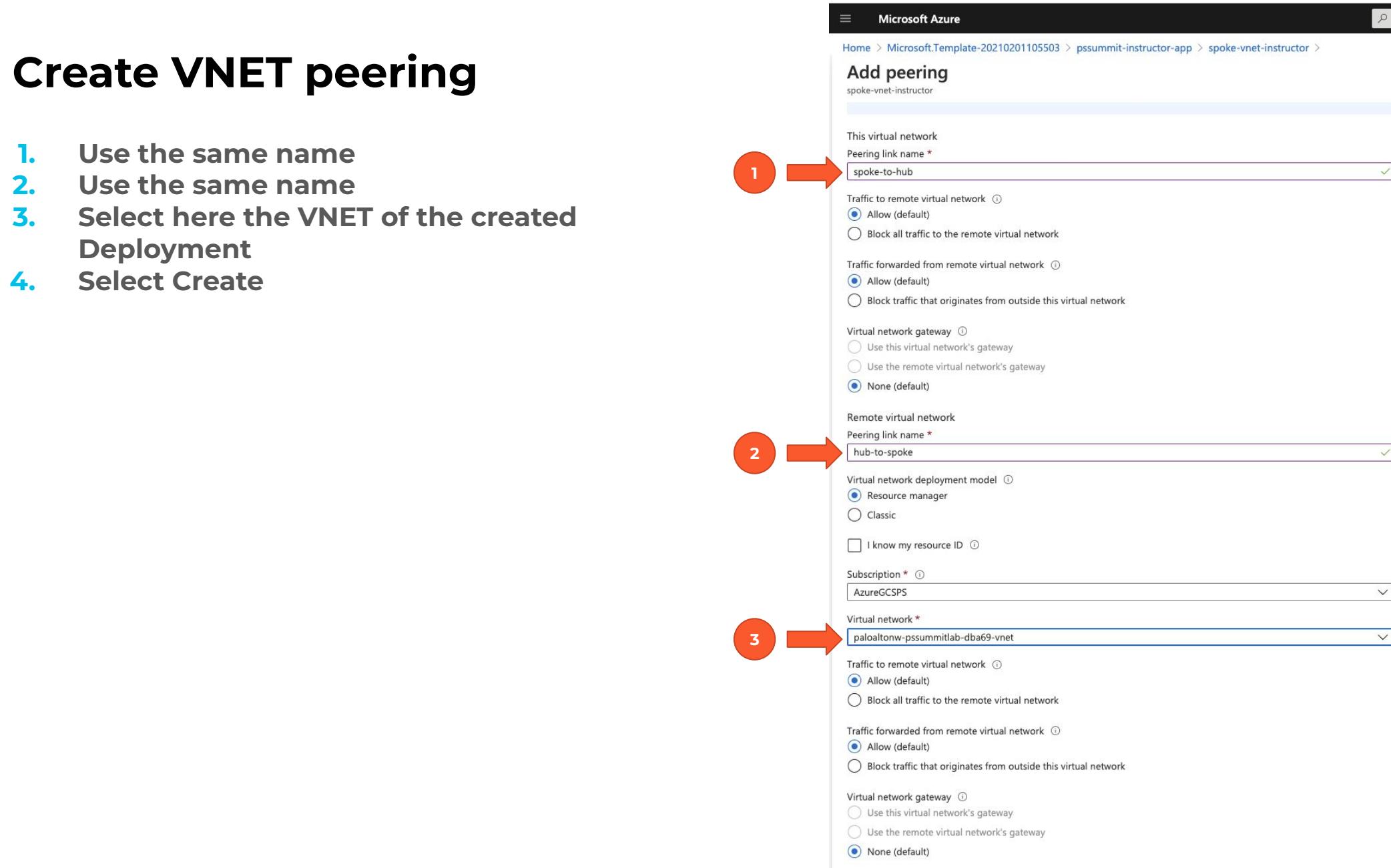
Virtual network * ▼

Traffic to remote virtual network ⓘ
 Allow (default)
 Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ
 Allow (default)
 Block traffic that originates from outside this virtual network

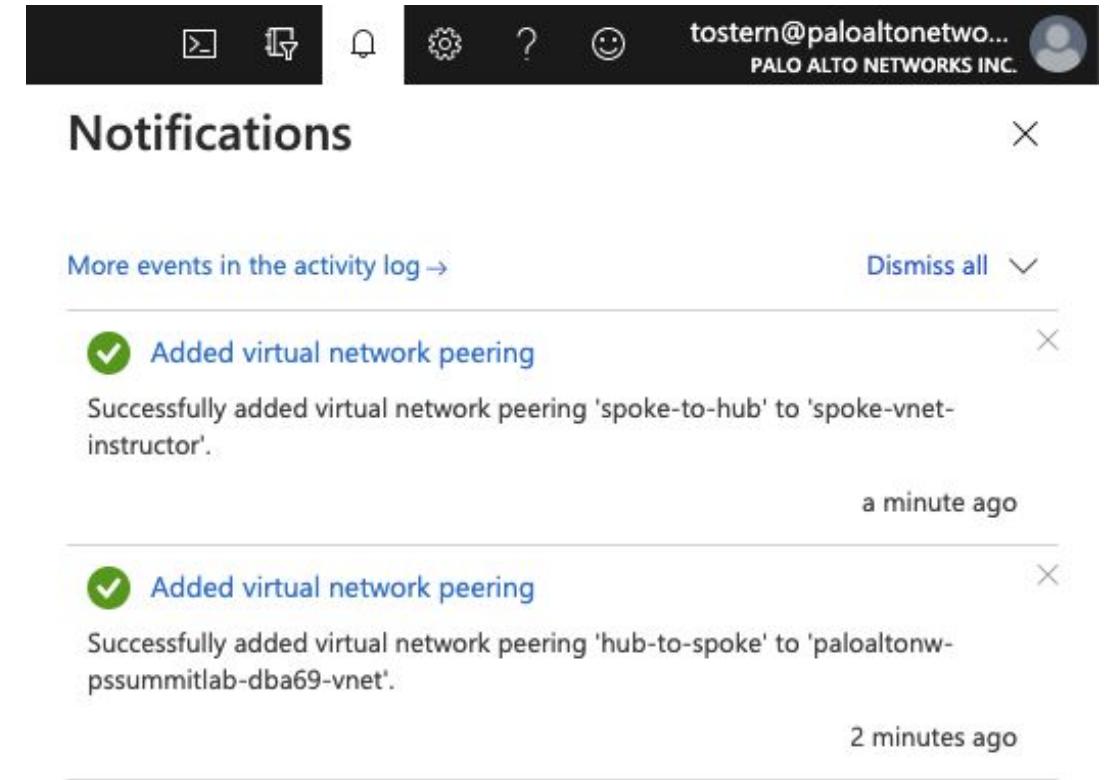
Virtual network gateway ⓘ
 Use this virtual network's gateway
 Use the remote virtual network's gateway
 None (default)

1 2 3



Validate VNET peering

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



The screenshot shows the Azure Notifications page with the following details:

- Header:** Includes icons for refresh, export, and settings, followed by a user profile for "tostern@paloaltonetwo..." from "PAO ALTO NETWORKS INC.".
- Title:** Notifications
- Actions:** A "Dismiss all" button with a dropdown arrow.
- Event 1:** **Added virtual network peering** (a minute ago)
Successfully added virtual network peering 'spoke-to-hub' to 'spoke-vnet-instructor'.
Details: [More events in the activity log](#)
- Event 2:** **Added virtual network peering** (2 minutes ago)
Successfully added virtual network peering 'hub-to-spoke' to 'paloaltonw-pssummitlab-dba69-vnet'.
Details: [More events in the activity log](#)

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

The screenshot shows the PANORAMA web interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is selected), OBJECTS, NETWORK, DEVICE, and PANORAMA. On the left, a sidebar menu is open under the Security section, showing Pre Rules, Post Rules, and Default Rules. Below this, NAT and QoS sections are also visible. The main content area displays a table of security rules. The table has columns for NAME, LOCATION, TAGS, TYPE, Source (Zone, Address, User, Device), Destination (Zone, Address, Device), APPLICATION, SERVICE, ACTION, PROFILE, OPTIONS, TARGET, and RULE USAGE. There are two entries in the table:

NAME	LOCATION	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	TARGET	RULE USAGE
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE							
1 azure health probe	Outbound-Stack	none	universal	[pan-data-zone]	[pan-azure-hea...]	any	any	[pan-data-zone]	any	any	any	application-...	Allow	[edit]	[profile]	any	Used
2 allow-any	Outbound-Stack	none	universal	[pan-data-zone]	any	any	any	[pan-data-zone]	any	any	any	application-...	Allow	[edit]	[profile]	any	Used

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

Microsoft Azure

Home > Microsoft.Template-20210201105503 > pssummit-instructor-app > New > Route table >

Create Route table

Basics Tags Review + create

Project details

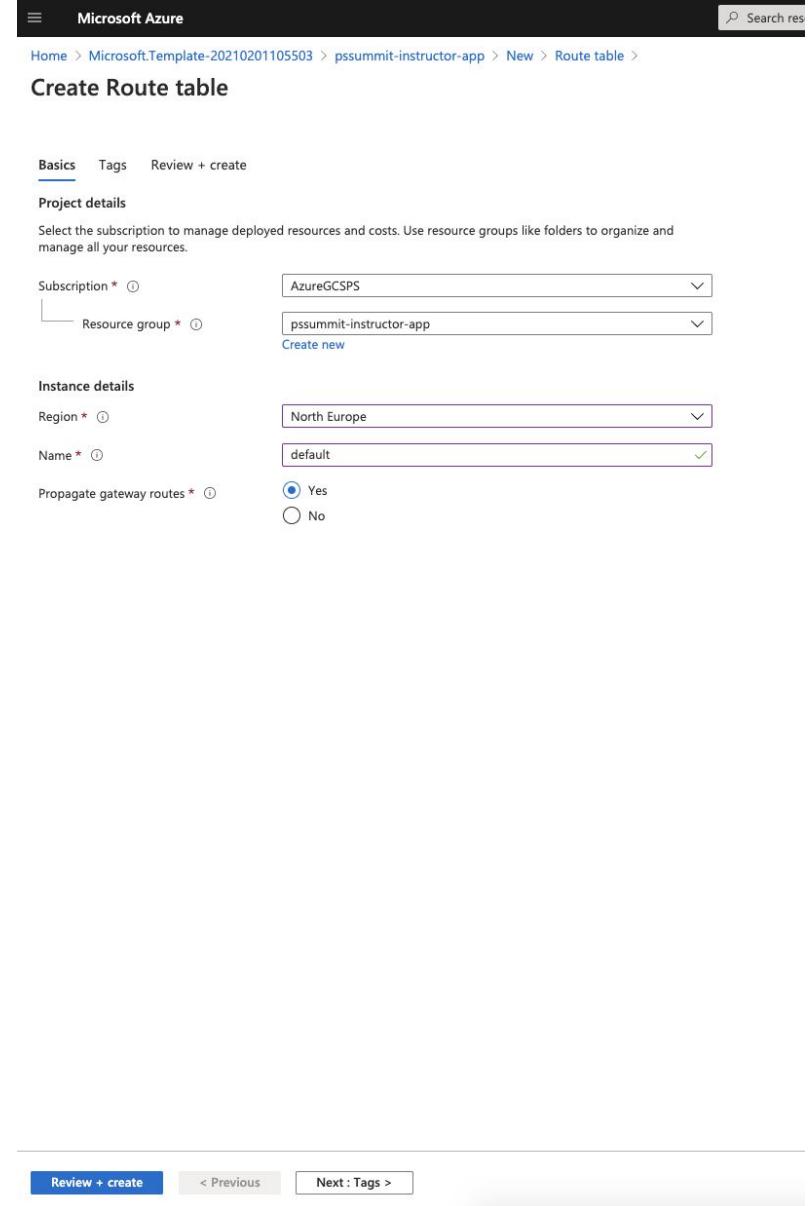
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Resource group * [Create new](#)

Instance details

Region * Name * Propagate gateway routes * Yes No

[Review + create](#) [Next : Tags >](#)



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

The screenshot shows the Microsoft Azure portal interface for managing a route table. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information. The main navigation bar on the left lists 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings', 'Configuration', 'Routes', and 'Subnets'. The 'Subnets' item is currently selected and highlighted in grey. The main content area displays a table of subnets associated with the route table. A search bar at the top of the table allows filtering by name, address range, virtual network, and security group. One subnet is listed: 'spoke-vnet-subnet-instructor' with address range '10.212.1.0/25', associated with 'spoke-vnet-instructor' and 'default-NSG'. A prominent blue 'Associate' button is located above the table. A dropdown menu is open over this button, showing the same subnet entry: 'spoke-vnet-subnet-instructor'.

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓
spoke-vnet-subnet-instructor	10.212.1.0/25	spoke-vnet-instructor	default-NSG

Create static Route

1. Select Routes
2. Click Add

Microsoft Azure

Search resources, services, and docs (G+/)

tostern@paloaltonetwo...
PALO ALTO NETWORKS INC.

Home > Microsoft.RouteTable-20210201111953 > pssummit-instructor-app > default

default | Routes

Route table

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

+ Add

Search routes

Name	Address prefix	Next hop type
------	----------------	---------------

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

The screenshot shows the Microsoft Azure portal interface for editing a route. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information. Below the navigation is a breadcrumb trail: Home > Microsoft.RouteTable-20210201111953 > pssummit-instructor-app > default >. The main content area is titled "Edit route" and shows a "default" route. There are three input fields with validation stars: "Address prefix" containing "0.0.0.0/0", "Next hop type" set to "Virtual appliance", and "Next hop address" containing "192.168.0.74". At the bottom are "Save", "Discard", and "Delete" buttons. Three red arrows with numbers 1, 2, and 3 point from the top of the image to the respective input fields.

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

Configure VM-Series

Interface Configuration

Log into FW1

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

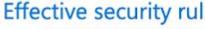
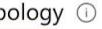
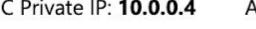
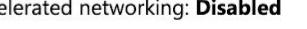
Home > PSSummitLAB > vmseries-vm1 - Networking

 **vmseries-vm1 - Networking**
Virtual machine

Search (Cmd+/) <>  Attach network interface  Detach network interface

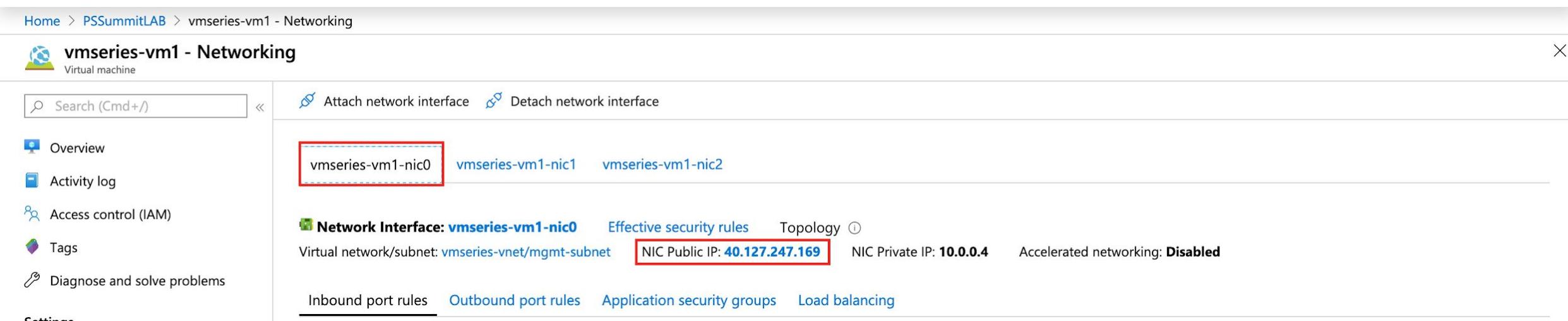
 Overview  Activity log  Access control (IAM)  Tags  Diagnose and solve problems

vmseries-vm1-nic0  

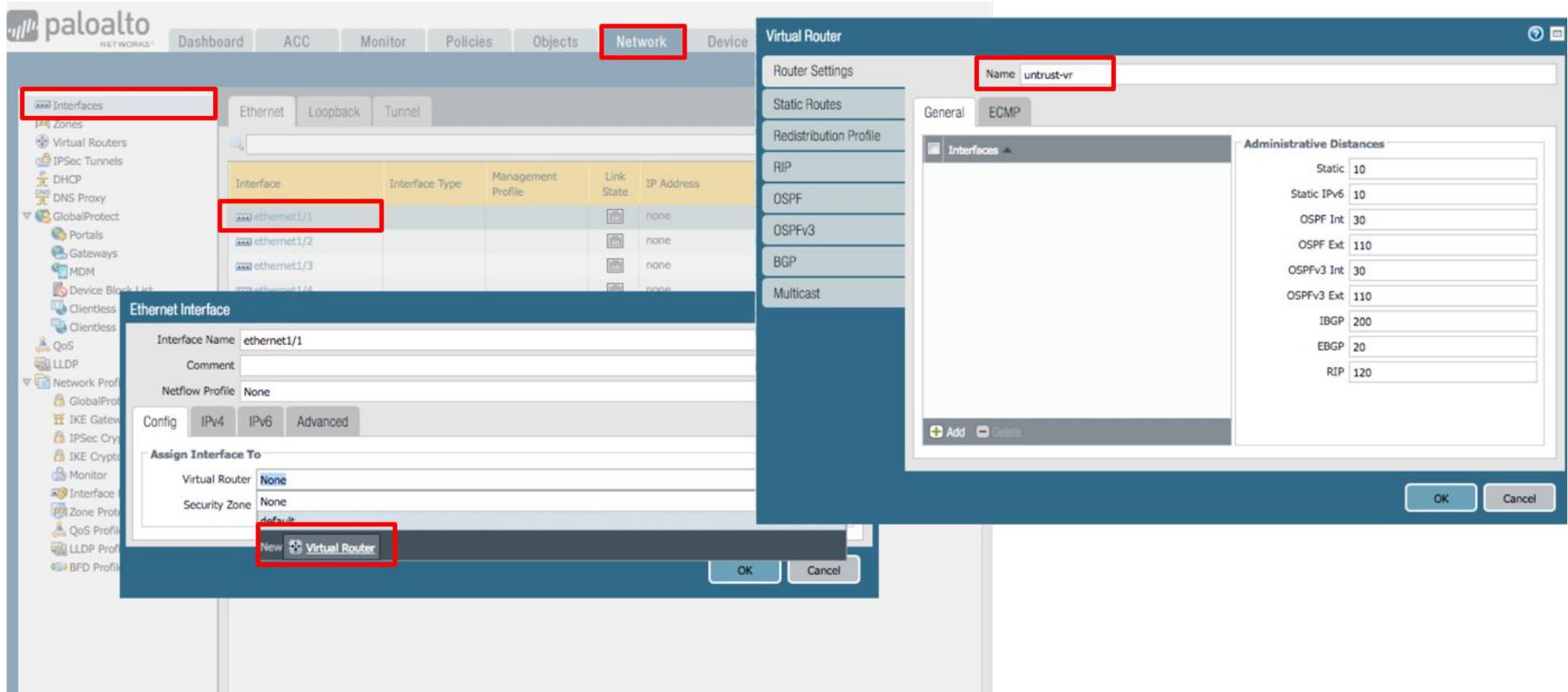
 **Network Interface:** **vmseries-vm1-nic0**  Effective security rules  Topology
Virtual network/subnet: **vmseries-vnet/mgmt-subnet**  NIC Public IP: **40.127.247.169**  NIC Private IP: **10.0.0.4**  Accelerated networking: **Disabled**

Inbound port rules  Outbound port rules  Application security groups 

Settings



Configure Untrust Interface - Virtual Router



Configure Untrust Interface - Zone

The screenshot displays two overlapping configuration windows from the Palo Alto Networks Management Console.

Left Window: Ethernet Interface Configuration

- Interface Name:** ethernet1/1
- Comment:** (empty)
- Netflow Profile:** None
- Config Tab:** Selected
- Assign Interface To:**
 - Virtual Router:** untrust-vr
 - Security Zone:** None (highlighted with a red box)
 - New Zone:** (button highlighted with a red box)

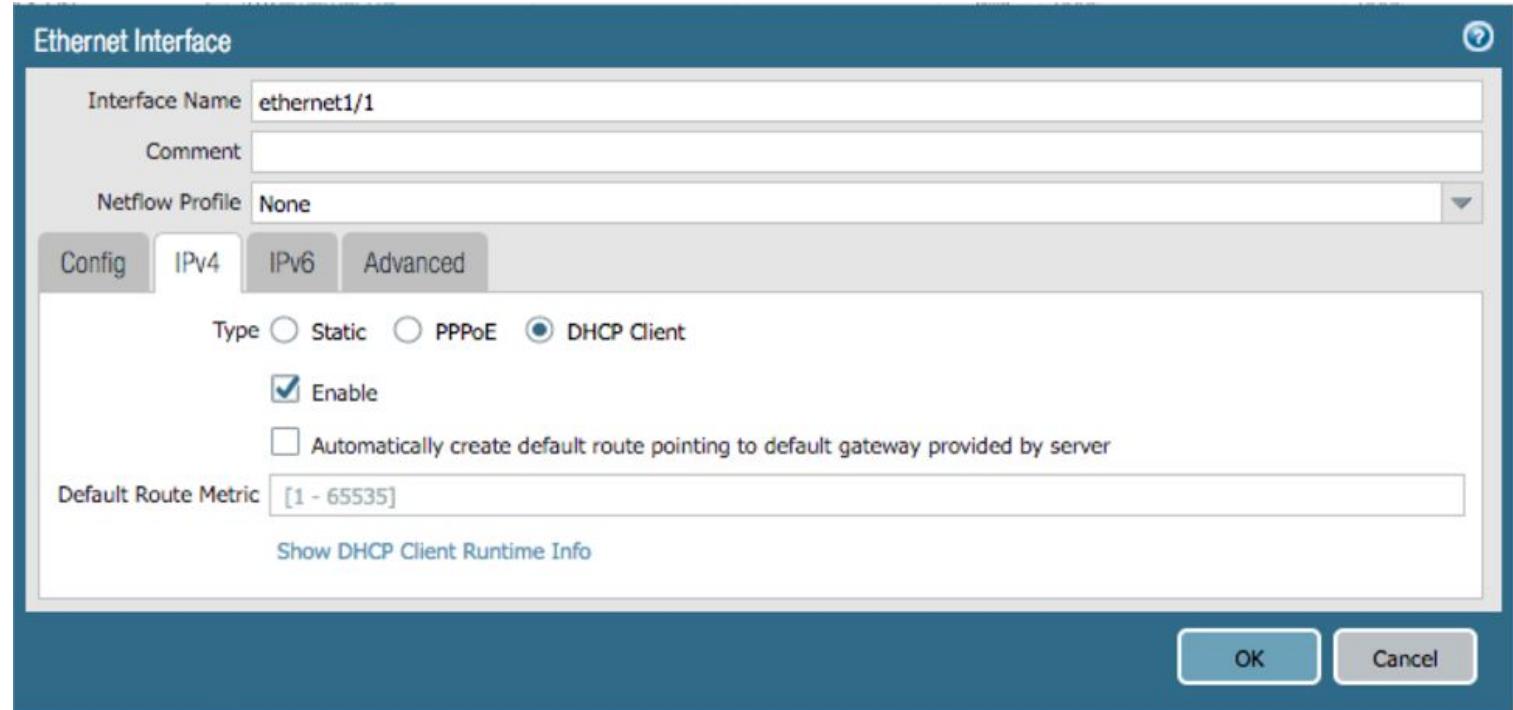
Right Window: Zone Configuration

- Name:** untrust-zone (highlighted with a red box)
- Type:** Layer3
- User Identification ACL:**
 - Include List:** (empty)
 - Add:** (button)
 - Delete:** (button)
 - Description:** Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
- Zone Protection:**
 - Zone Protection Profile:** None
 - Enable Packet Buffer Protection:** (checkbox)
- Exclude List:**
 - Add:** (button)
 - Delete:** (button)
 - Description:** Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Buttons: OK, Cancel

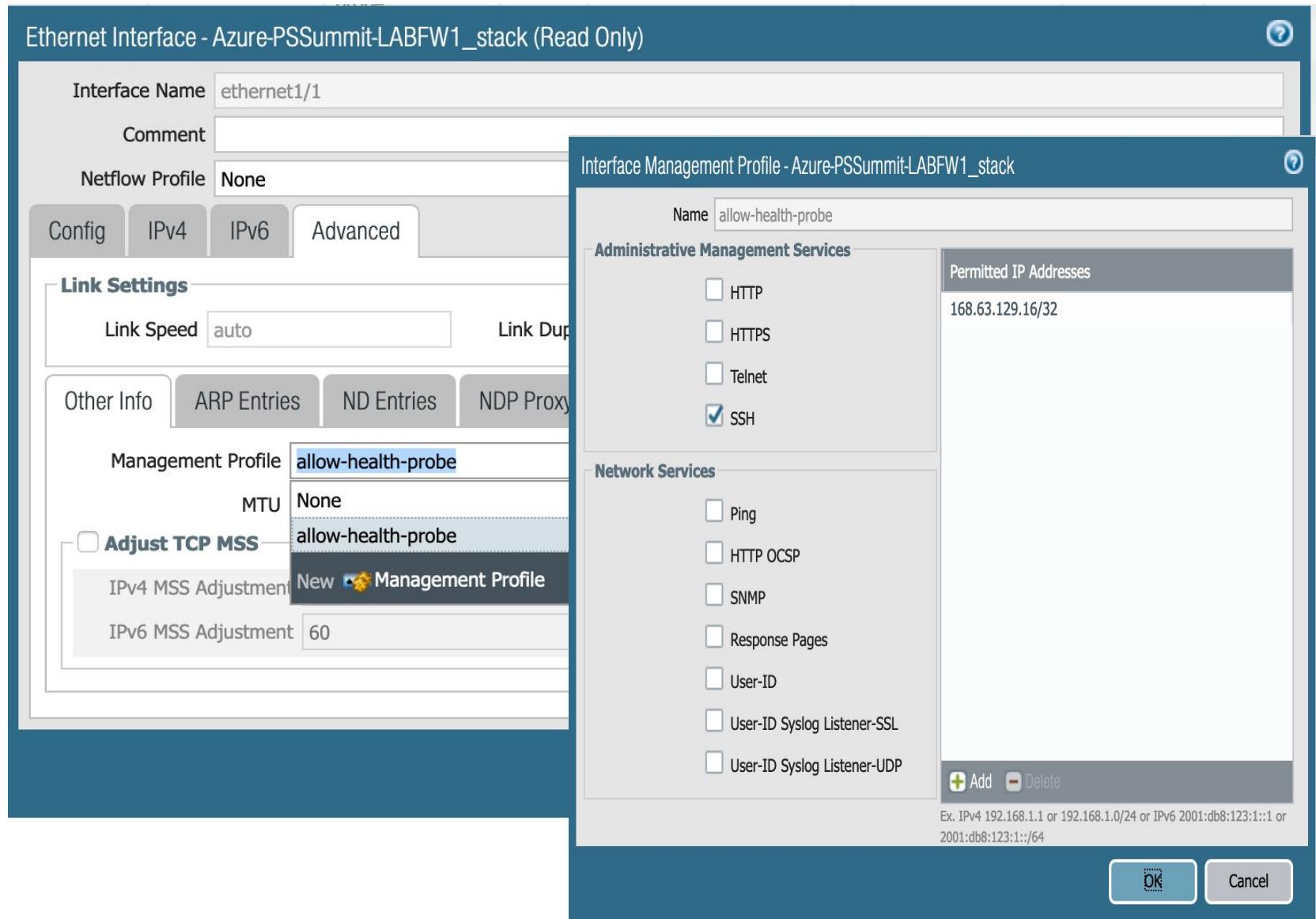
Configure Untrust Interface - DHCP

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

The screenshot shows the Palo Alto Networks UI interface for configuring a Trust interface on a Virtual Router.

Left Sidebar: Shows navigation links for Interfaces, Zones, Virtual Routers, IPsec Tunnels, DHCP, DNS, GlobalProtect, Portals, Gateways, MDM, Device Block List, Clientless, Clientless, QoS, LLDP, Network Profiles, GlobalProtect, IKE Gateways, IPsec Cryptos, IKE Cryptos, Monitor, Interface Types, Zone Protocols, QoS Profiles, LLDP Profiles, and BFD Profiles.

Main View (Interfaces Tab): Shows a table of interfaces. An interface named "ethernet1/2" is selected and highlighted with a red box. The table columns include Interface, Interface Type, Management Profile, and Link State.

Virtual Router Configuration:

- Name:** trust-vr (highlighted with a red box)
- General Tab:** Shows the selected interface "ethernet1/2".
- ECMP Tab:** Shows the "Interfaces" section with an "Add" button and a "Delete" button.
- Administrative Distances:** A table listing administrative distances for various protocols.
- Buttons:** OK and Cancel.

Protocol	Administrative Distance
Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Bottom Bar: Shows "New Virtual Router" (highlighted with a red box).

Configure Trust Interface - Zone

Ethernet Interface

Interface Name: ethernet1/2

Comment:

Netflow Profile: None

Config IPv4 IPv6 Advanced

Assign Interface To

Virtual Router: trust-vr

Security Zone: **None**

None
untrust-zone

New **Zone**

Zone

Name: **trust-zone**

Log Setting: None

Type: Layer3

User Identification ACL

Enable User Identification

Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add **Delete**

Users from these addresses/subnets will be identified.

Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add **Delete**

Users from these addresses/subnets will not be identified.

OK Cancel

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”

Ethernet Interface - Azure-PSSummit-LABFW1_stack (Read Only)

Interface Name: ethernet1/2

Comment:

Netflow Profile: None

Config IPv4 IPv6 Advanced

Assign Interface To

Virtual Router: trust-vr

Security Zone: trust-zone

Ethernet Interface - Azure-PSSummit-LABFW1_stack (Read Only)

Interface Name: ethernet1/2

Comment:

Netflow Profile: None

Config IPv4 IPv6 Advanced

Type: Static PPPoE DHCP Client

Enable

Automatically create default route pointing to default gateway provided by server

Default Route Metric: [1 - 65535]

Show DHCP Client Runtime Info

OK Cancel

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

The screenshot shows two overlapping windows from a network configuration interface.

Main Window (Left): Ethernet Interface - Azure-PSSummit-LABFW1_stack (Read Only)

- Interface Name:** ethernet1/2
- Comment:** (empty)
- Netflow Profile:** None
- Tab Selection:** Advanced (selected)
- Link Settings:** Link Speed: auto, Link Duplex: (disabled)
- Other Info:** ARP Entries, ND Entries, NDP Proxy
- Management Profile:** allow-health-probe (selected)
- MTU:** None
- Adjust TCP MSS:** (checkbox is off) IPv4 MSS Adjustment: New Management Profile, IPv6 MSS Adjustment: 60

Modals (Right): Interface Management Profile - Azure-PSSummit-LABFW1_stack

- Name:** allow-health-probe
- Administrative Management Services:** HTTP, HTTPS, Telnet, SSH (SSH is checked)
- Permitted IP Addresses:** 168.63.129.16/32
- Network Services:** Ping, HTTP OCSP, SNMP, Response Pages, User-ID, User-ID Syslog Listener-SSL, User-ID Syslog Listener-UDP
- Buttons:** Add, Delete, OK, Cancel

At the bottom of the main window, there is a note: Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

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

The screenshot shows the Palo Alto Networks Firewall UI interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network (selected), Device, Commit, and Config.

The left sidebar menu lists various network components: Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, DHCP, DNS, GlobalProtect, Port Groups, Gateways, MDNs, Devs, Clients, QoS, LLDP, Networks (selected), IKE, IPSec, IKEv2, Multicast, and BFD.

The main content area displays a table of virtual routers:

Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runti...
trust-vr	ethernet1/2	ECMP status: Disabled						More Stats
untrust-vr	ethernet1/1	ECMP status: Disabled						More Stats

A modal dialog titled "Virtual Router - untrust-vr" is open, showing the "Static Routes" tab under "Router Settings". The "IPv4" tab is selected, displaying an empty table for static routes:

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
0 items								

At the bottom of the modal are buttons for "Add", "Delete", and "Clone". Below the modal are "OK" and "Cancel" buttons.

Configure Untrust VR - Static Routes

Virtual Router - Static Route - IPv4

Name	default
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	IP Address 10.0.1.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Virtual Router - Static Route - IPv4

Name	to-spoke1
Destination	172.17.0.0/16
Interface	None
Next Hop	Next VR trust-vr
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Virtual Router - Static Route - IPv4

Name	to-spoke2
Destination	192.168.0.0/16
Interface	None
Next Hop	Next VR trust-vr
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Configure Untrust VR - Static Routes Summary

Virtual Router - untrust-vr

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4

IPv6

3 items

Name	Destination	Interface	Next Hop		Admin Distance	Metric	BFD	Route Table
			Type	Value				
default	0.0.0.0/0	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast
to-spoke1	172.17.0.0/16		next-vr	trust-vr	default	10	None	unicast
to-spoke2	192.168.0.0/16		next-vr	trust-vr	default	10	None	unicast

Add Delete Clone

OK Cancel

The screenshot shows the 'Static Routes' configuration page for the 'untrust-vr' virtual router. The left sidebar lists various routing protocols. The main area displays three static routes under the 'IPv4' tab. Each route is defined by a name, destination, and next hop (either an interface or another virtual router). The routes are categorized under a 'Route Table' column. At the bottom, there are buttons for adding, deleting, or cloning routes.

Configure Trust VR

Go to:

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

The screenshot displays the Palo Alto Networks Firewall UI. The top navigation bar includes Dashboard, ACC, Monitor, Policies, Objects, Network (selected), Device, Commit, and Config. The left sidebar lists various network components: Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, DHCP, DNS, GlobalRPs, Port, Gate, MDI, Dev, Client, QoS, LLDP, Network (selected), IKE, IPSec, IKE, Multicast, and BFD. The main content area shows two virtual routers: trust-vr and untrust-vr. The untrust-vr router is selected, and its configuration pane is open. The configuration pane title is "Virtual Router - untrust-vr". It contains tabs for Router Settings, Static Routes (selected), Redistribution Profile, RIP, OSPF, OSPFv3, BGP, and Multicast. Under Static Routes, there are tabs for IPv4 and IPv6. The IPv4 tab shows a table with columns: Name, Destination, Interface, Type, Value, Admin Distance, Metric, BFD, and Route Table. The table currently has 0 items. At the bottom of the configuration pane are buttons for Add, Delete, and Clone. Below the configuration pane are OK and Cancel buttons.

Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runti
trust-vr	ethernet1/2	ECMP status: Disabled						
<input checked="" type="checkbox"/> untrust-vr	ethernet1/1	ECMP status: Disabled						

Virtual Router - untrust-vr

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4

IPv6

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
0 items								

Add Delete Clone

OK Cancel

Configure Trust VR - Static Routes

Virtual Router - Static Route - IPv4

Name	default
Destination	0.0.0.0/0
Interface	None
Next Hop	Next VR
	untrust-vr
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Virtual Router - Static Route - IPv4

Name	LB
Destination	168.63.129.16/32
Interface	ethernet1/2
Next Hop	IP Address
	10.0.2.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Virtual Router - Static Route - IPv4

Name	spoke-2
Destination	192.168.0.0/16
Interface	ethernet1/2
Next Hop	IP Address
	10.0.2.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Virtual Router - Static Route - IPv4

Name	spoke-1
Destination	172.17.0.0/16
Interface	ethernet1/2
Next Hop	IP Address
	10.0.2.1
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Configure Trust VR - Static Routes

Virtual Router - trust-vr

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4

IPv6

Name	Destination	Interface	Next Hop		Admin Distance	Metric	BFD	Route Table
			Type	Value				
default	0.0.0.0/0		next-vr	untrust-vr	default	10	None	unicast
spoke-1	172.17.0.0/16	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
spoke-2	192.168.0.0/16	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
<input checked="" type="checkbox"/> internal-lb-probe	168.63.129.16/32	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast

+ Add - Delete Clone

OK Cancel

Repeat these steps on FW2 using the
same settings

Configure NAT & Security Policies

NAT Policy Overview

The screenshot shows the Palo Alto Networks Panorama interface. The top navigation bar includes links for Dashboard, ACC, Monitor, Policies (which is highlighted with a red box), Objects, Network, and Device. A dropdown menu for the device 'PSSummit-LAB-FW1' is visible. On the left, a sidebar under the 'Security' heading lists NAT (also highlighted with a red box), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and Dos Protection. The main content area displays a table of NAT policies:

ID	Name	Tags	Original Packet						Translated Packet		Rule Usage		
			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	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-https	dynamic-ip-and-port ethernet1/2	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	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	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 Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Name: No-NAT-Azure-Probe
Description:
Tags: Azure
Group Rules By Tag: Azure
NAT Type: ipv4
Audit Comment:

Audit Comment Archive

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Zone: untrust-zone

Destination Zone: untrust-zone

Source Address: Azure-Health-Probe

Destination Address: Any

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Address Translation: Translation Type: None

Destination Address Translation: Translation Type: None

OK Cancel

NAT Policy for VM Jumphost

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

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Name: Inbound-jump-VM-Spoke2
Description:
Tags: Inbound
Group Rules By Tag: None
NAT Type: ipv4
Audit Comment:

Audit Comment Archive

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Zone: untrust-zone
Destination Zone: untrust-zone
Source Address: Any
Destination Address: Any
Destination Interface: any
Service: ssh

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Address Translation
Translation Type: Dynamic IP And Port
Address Type: Interface Address
Interface: ethernet1/2
IP Type: IP
None

Destination Address Translation
Translation Type: Dynamic IP (with session distribution)
Translated Address: 172.17.0.4
Translated Port: 22
Session Distribution Method: Round Robin

OK Cancel

NAT Policy for the Webserver

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

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Name: Inbound-Webserver-Spoke1
Description:
Tags: Inbound
Group Rules By Tag: None
NAT Type: ipv4
Audit Comment:
Audit Comment Archive

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Zone: untrust-zone
Destination Zone: untrust-zone
Source Address: Any
Destination Address: Any

Destination Interface: any
Service: service-http

Add Delete Add Delete OK Cancel

NAT Policy Rule

General Original Packet Translated Packet Active/Active HA Binding Target

Source Address Translation:

- Translation Type: Dynamic IP And Port
- Address Type: Interface Address
- Interface: ethernet1/2
- IP Type: IP
- None

Destination Address Translation:

- Translation Type: Dynamic IP (with session distribution)
- Translated Address: 192.168.0.4
- Translated Port: 80
- Session Distribution Method: Round Robin

OK Cancel

NAT Policy: outbound-internet-nat

NAT Policy Rule

General Original Packet Translated Packet

Name: internet

Description:

Tags:

NAT Type: ipv4

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Zone: trust-zone

Destination Zone: untrust-zone

Source Address:

Destination Address:

Destination Interface: any

Service: any

Add Delete Add Delete Add Delete

OK Cancel

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/2

IP Address: None

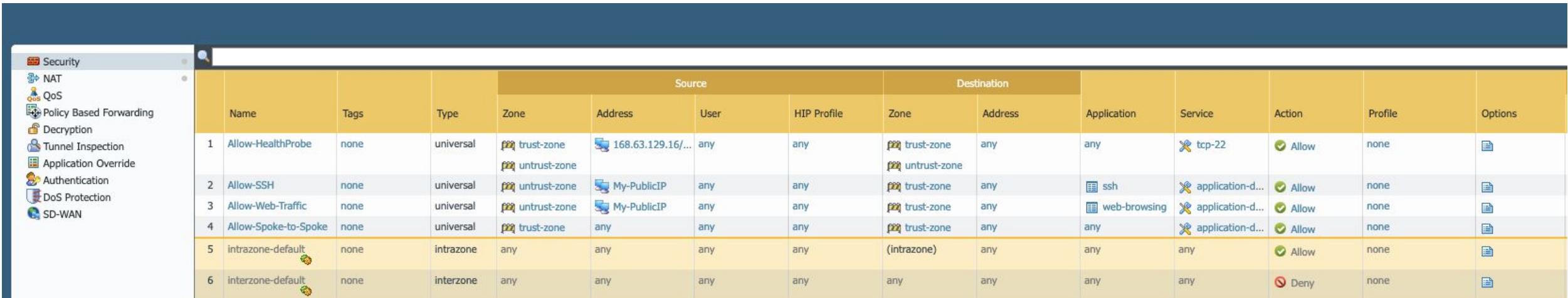
Destination Address Translation

Translation Type: None

OK Cancel

Create Limited Security rules

Replace “My-PublicIP” with your yours



The screenshot shows the Palo Alto Networks Firewall configuration interface. On the left, a sidebar lists various security features: NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main area displays a table of security rules.

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	Edit
2 Allow-SSH	none	universal	untrust-zone	My-PublicIP	any	any	trust-zone	any	ssh	application-d...	Allow	none	Edit
3 Allow-Web-Traffic	none	universal	untrust-zone	My-PublicIP	any	any	trust-zone	any	web-browsing	application-d...	Allow	none	Edit
4 Allow-Spoke-to-Spoke	none	universal	trust-zone	any	any	any	trust-zone	any	any	application-d...	Allow	none	Edit
5 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	Edit
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	Edit

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

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with the 'All resources' option highlighted by a red box. The main content area shows the 'All resources' blade for the 'firewall-public-lb' resource group. A second red box highlights the 'firewall-public-lb' entry in the list. On the right, the detailed view for the 'firewall-public-lb' load balancer is displayed. The 'Overview' tab is selected. Key details shown include:

Setting	Value
Resource group (change)	palo-test-rg
Location	East US
Subscription name (change)	Visual Studio Professional
Subscription ID	36a6952c-125c-4b32-943e-27e85b91d591
SKU	Standard
Public IP address	104.45.173.74 (public-lb-pip)

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 ping 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 ping 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

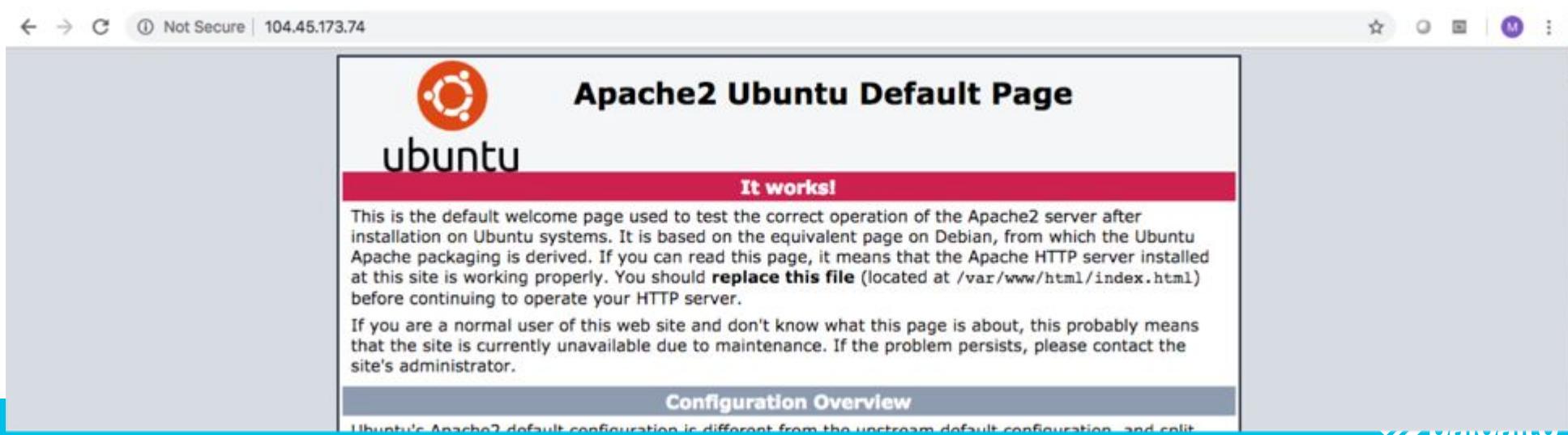
While in the jump-vm, SSH to the Web-VM in Spoke-2-VNET

```
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.

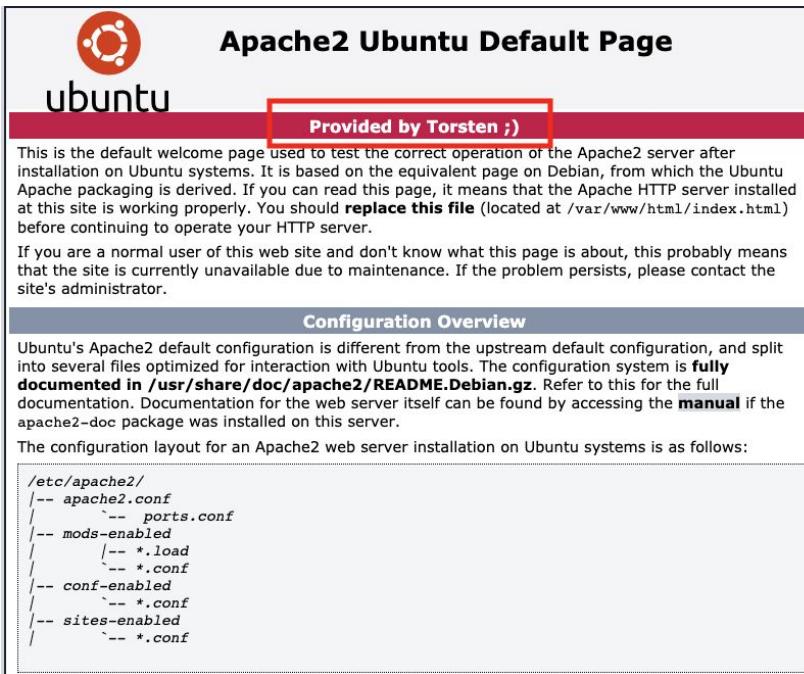
The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor (which is highlighted with a red box), Policies, Objects, Network, and Device. To the right are buttons for Commit, Config, and Search. Below the navigation is a toolbar with various icons. On the left, a sidebar under the 'Logs' heading has a 'Traffic' item selected (also highlighted with a red box). A search bar at the top of the main content area contains the filter '(addr in 192.168.0.4)'. The main pane displays a table of traffic logs with the following columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, and Action. Five log entries are listed:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Action	Application	Action
11/12 14:42:42	end	trust-zone	untrust-zone	192.168.0.4		91.189.89.199	123	allow	ntp	allow
11/12 14:37:15	end	trust-zone	trust-zone	172.17.0.4		192.168.0.4	22	allow	ssh	allow
11/12 14:31:49	end	trust-zone	untrust-zone	192.168.0.4		52.168.50.79	80	allow	apt-get	allow
11/12 14:31:24	end	trust-zone	untrust-zone	192.168.0.4		91.189.95.15	80	allow	web-browsing	allow
11/12 14:30:44	end	trust-zone	trust-zone	172.17.0.4		192.168.0.4	0	allow	ping	allow

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

