



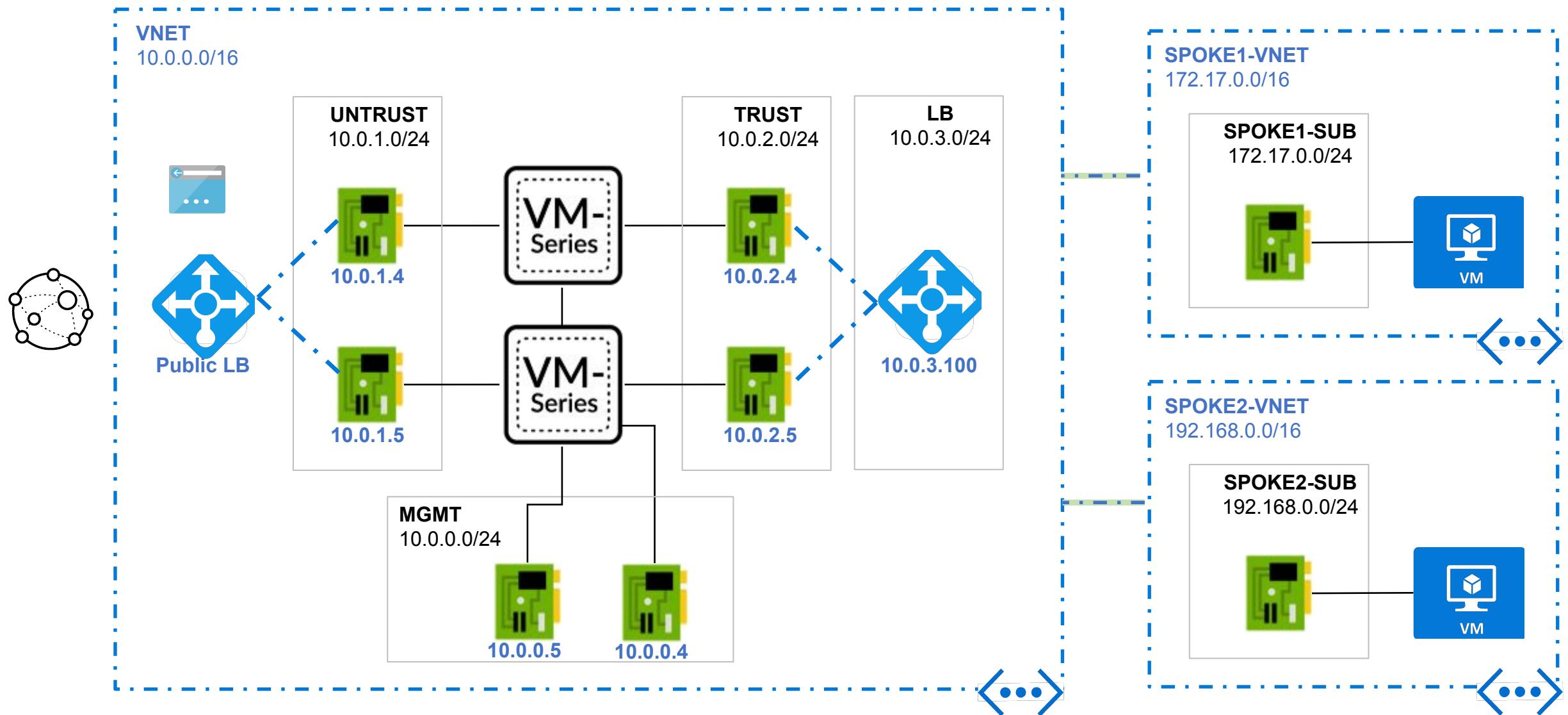
Prisma Public Cloud - Azure

Lab Guide

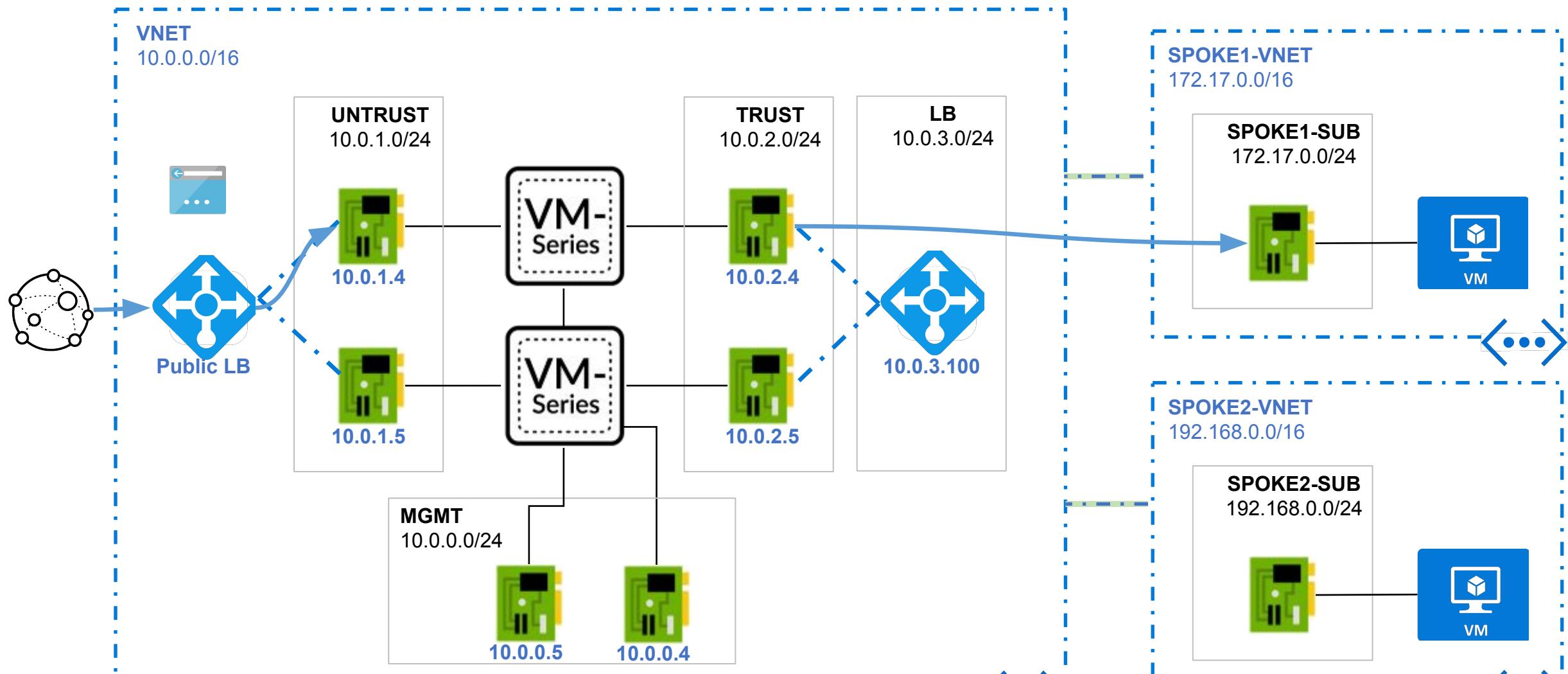


Lab Design

Overall Design

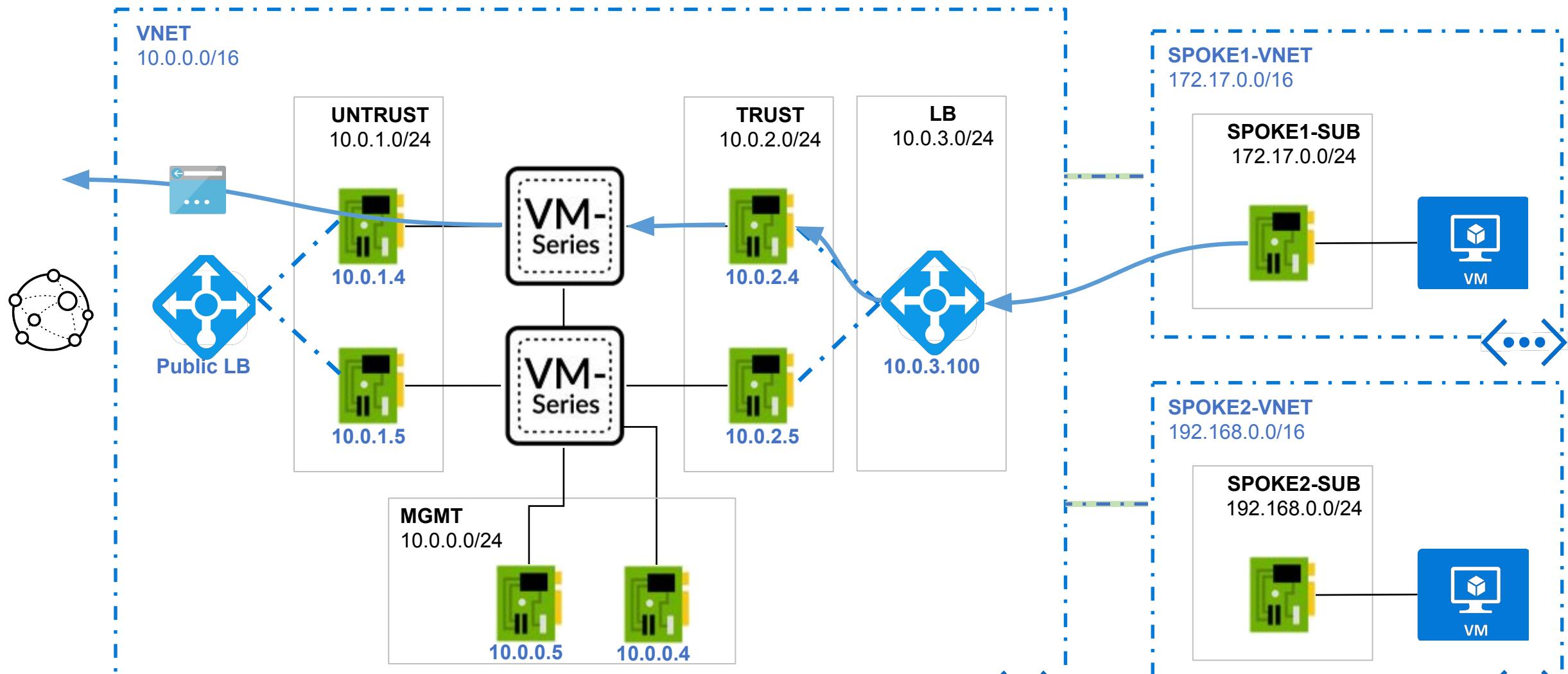


INBOUND TRAFFIC FLOW



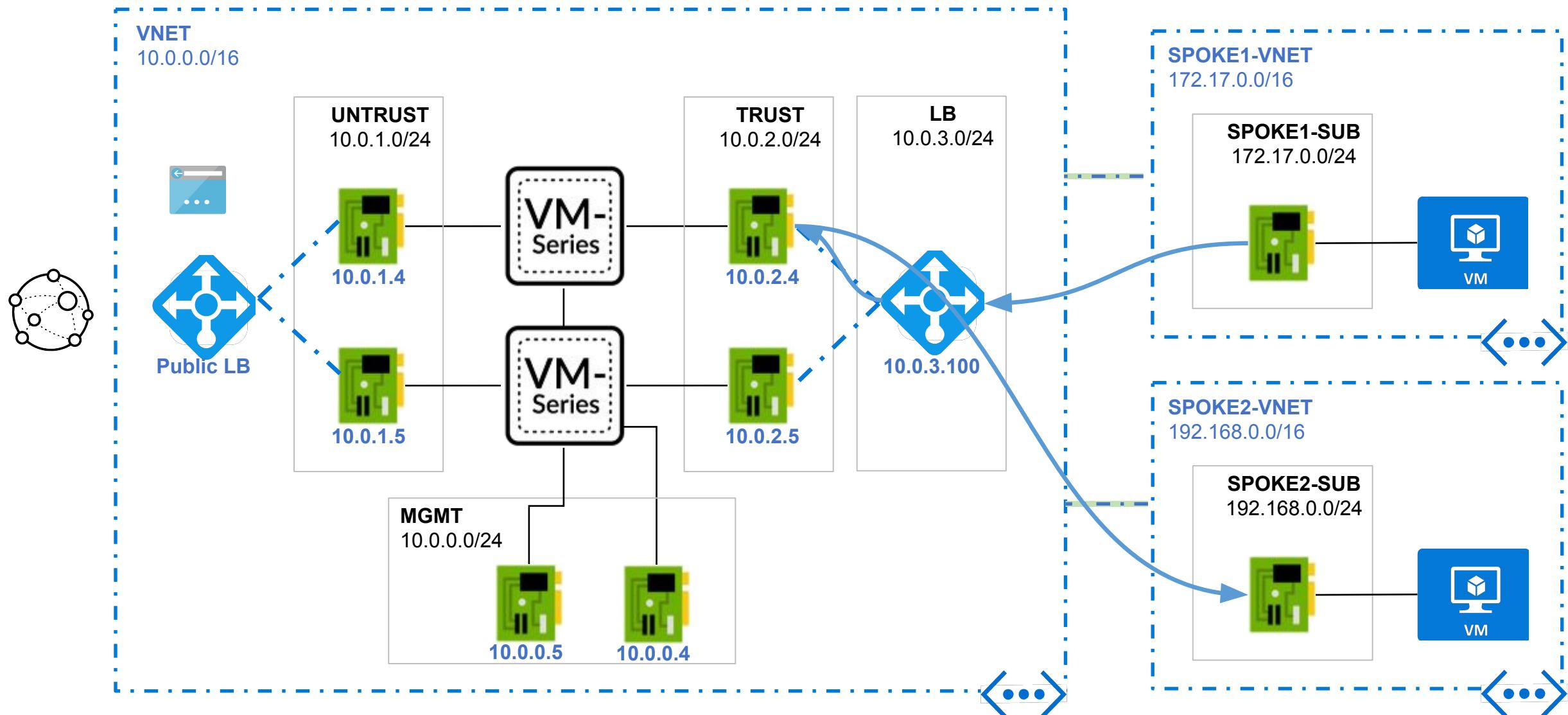
	Name	Tags	Original Packet							Translated Packet	
			Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service		Source Translation	Destination Translation
2	inbound-spoke1	none	untrust-zone	untrust-zone	any	any	untrust-nic	any		dynamic-ip-and-port	destination-translation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

OUTBOUND TRAFFIC FLOW



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



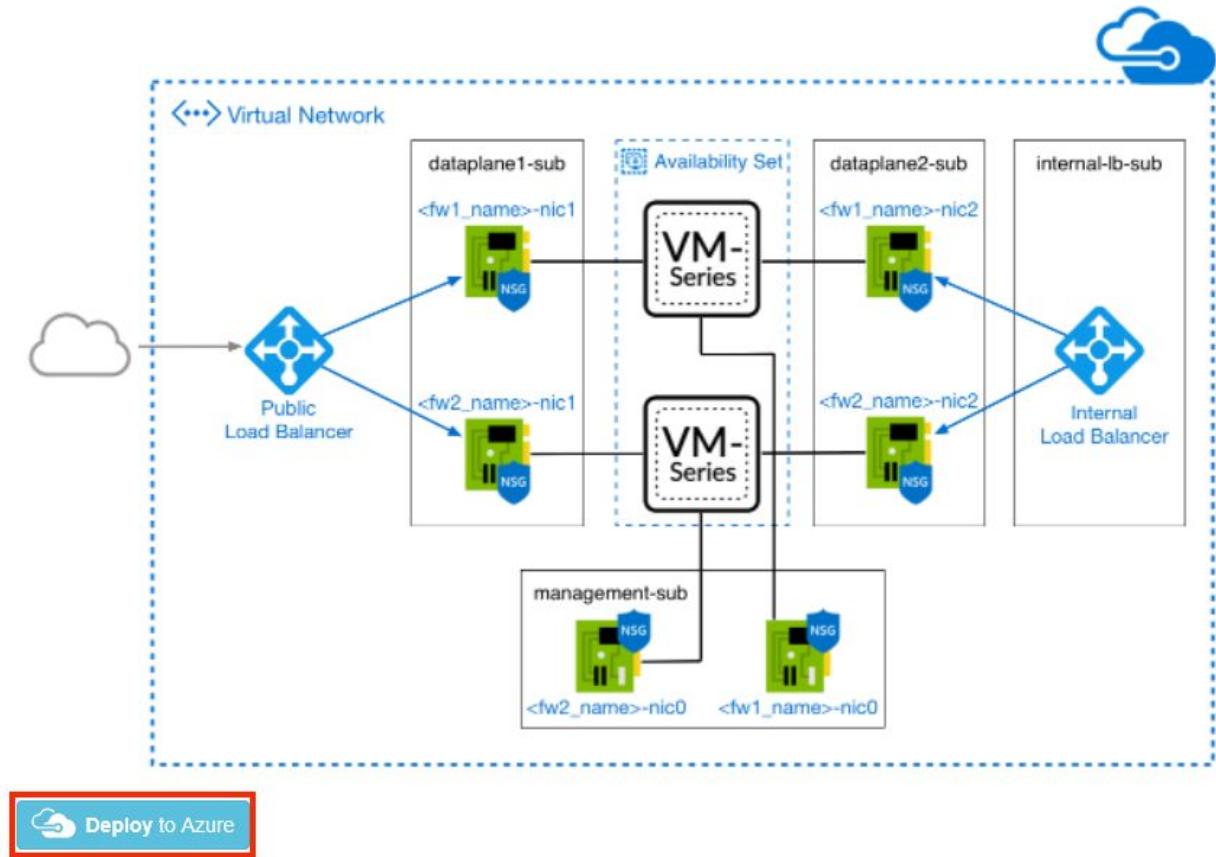
Deploy environment

Deploy Environment

1. Click on the Link

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

2. Click on “Deploy to Azure”



Deploy Environment 1/2

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

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 2/2

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

Admin/Admin2 is not a Valid Username

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

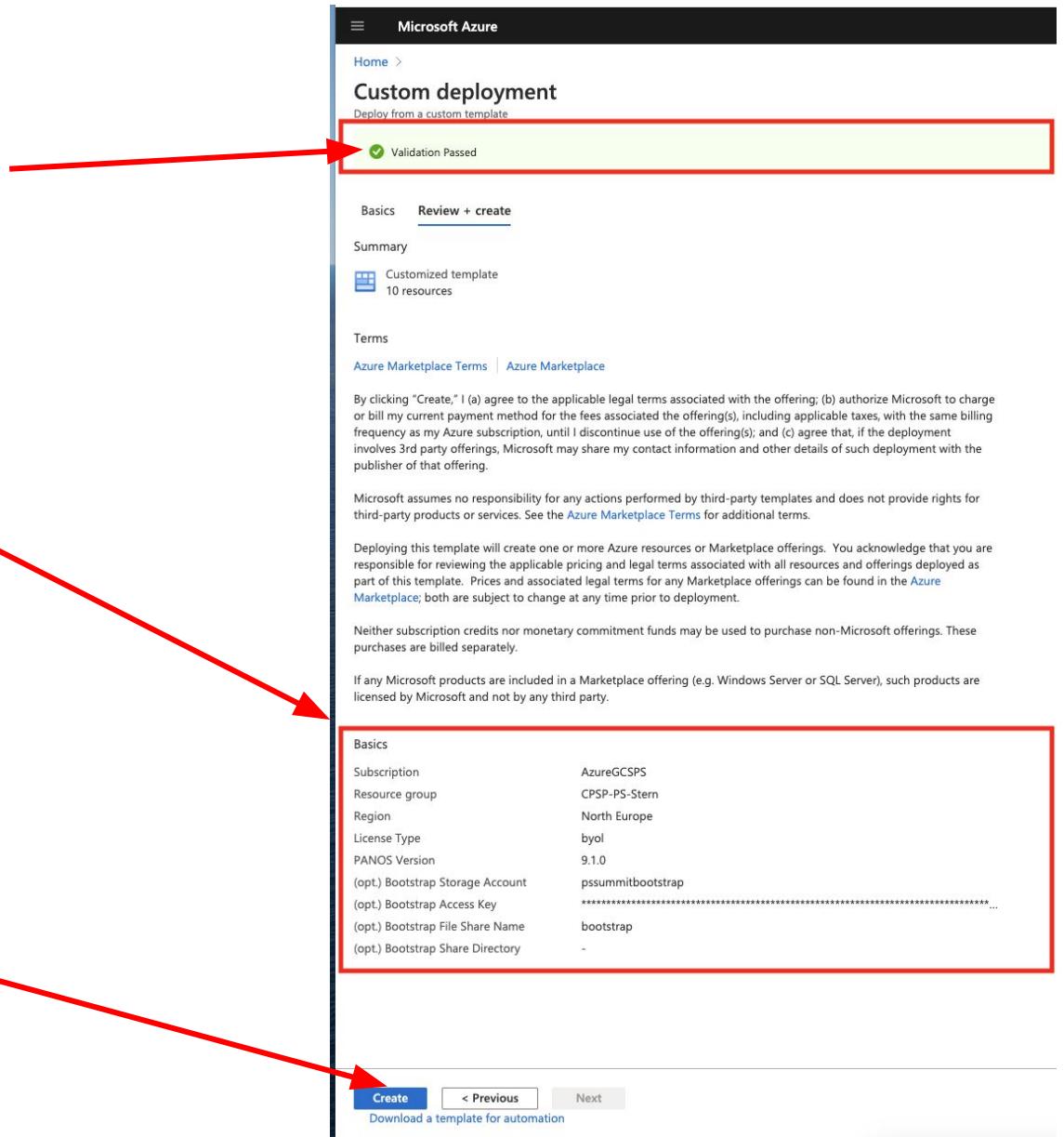
Next : Review + create >

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

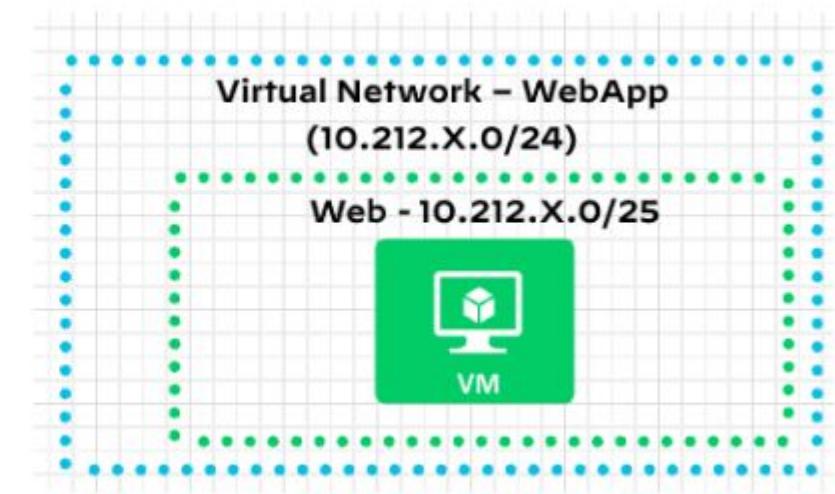
<https://github.com/PaloAltoNetworks/lab-azure-vmseries>

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 [Edit](#)
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 * [Edit](#)
AzureGCSPS

Resource group * [Edit](#)
(New) PSSummit-Instructor-Spoke

[Create new](#)

Parameters

Region * [Edit](#)
North Europe

Admin Username * [Edit](#)
fwadmin

Admin Password * [Edit](#)
.....

VNET Option [Edit](#)
Create new VNET

VNET Resource Group [Edit](#)

Vm Name [Edit](#)
Web-App

Virtual Network Name [Edit](#)
spoke-vnet

Address Prefix [Edit](#)
10.212.1.0/24

Subnet Name [Edit](#)
spoke-vnet-subnet

Subnet Prefix [Edit](#)
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 a Route Table** in the Application Virtual Networks to forward traffic to the “Egress Private IP” which is the Private IP of the Internal Load Balancer.
 - For instance “0.0.0.0/0” to “Egress Private IP” for Outbound / East-West Traffic
3. **Configure Web-App Server** to simulate a Web Server
 - Upgrade OS
 - Install Apache Web Server
 - Update Websites unique per Student

Configure VM-Series

Login into your Firewall

Login into VM-Series Firewall

- Go to your Resource Group you created in [Slide 9](#)
- Click on the first VM-Series firewall

The screenshot shows the Microsoft Azure Resource Group Overview page for the 'Pre-Req-Lab-Instructor' resource group. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (tostern@paloaltonetwo...). Below the header, the resource group name 'Pre-Req-Lab-Instructor' is displayed along with its status as a 'Resource group'. The left sidebar contains sections for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, and Events. The main content area is titled 'Essentials' and displays subscription details: (move) to AzureGCSPS, Subscription ID d47f1af8-9795-4e86-bbce-da72cf0f8ec, Tags (edit) Click here to add tags, Deployments 8 Succeeded, Location North Europe. Below this, the 'Resources' section lists 21 records, showing columns for Name, Type, and Location. The listed resources include 'vnet-instructor' (Virtual network, North Europe), 'vmseries-fw-vm1' (Virtual machine, North Europe), and 'vmseries-fw-vm2' (Virtual machine, North Europe).

Name	Type	Location
vnet-instructor	Virtual network	North Europe
vmseries-fw-vm1	Virtual machine	North Europe
vmseries-fw-vm2	Virtual machine	North Europe

Login into VM-Series Firewall

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

The screenshot shows the Microsoft Azure portal interface for a virtual machine named "vmseries-fw-vm1". The "Overview" tab is selected on the left sidebar. At the top, there is a search bar and a navigation bar with icons for search, refresh, and user profile. Below the search bar, the VM name "vmseries-fw-vm1" is displayed along with its status "Running". A "Connect" button is available. The main content area displays the VM's details under the "Essentials" section. The "Public IP address" field is highlighted with a red box. The IP address shown is 52.33. The "JSON View" link is located at the bottom right of the essentials section.

Resource group	Pre-Req-Lab-Instructor
Status	Running
Location	North Europe
Subscription	A
Subscription ID	d
Tags	Click here to add tags
Operating system	: Linux (centos PanOS)
Size	: Standard DS3 v2 (4 vcpus, 14 GiB memory)
Public IP address	: 52.33
Virtual network/subnet	: vnet-instructor/mgmt-subnet
DNS name	: Not configured

Configure VM-Series

Interface Configuration

Configure Untrust Interface - IPv4

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

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (which is selected and highlighted in yellow), and DEVICE.

The left sidebar menu under the NETWORK tab includes: Interfaces, Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (with Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, and Network Profiles (with GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, and SD-WAN Interface Profile).

The main content area shows the Ethernet interface list with "ethernet1/1" selected. The "Ethernet Interface" configuration dialog is open, showing the following settings:

- Interface Name: ethernet1/1
- Comment: (empty)
- Interface Type: Layer3
- Netflow Profile: None
- Config tab is selected, showing:
 - Enable SD-WAN:
 - Type: Static PPPoE DHCP Client
 - Enable:
 - Automatically create default route pointing to default gateway provided by server:
 - Send Hostname: system-hostname
 - Default Route Metric: 10
- IPv4 tab is also visible.

At the bottom right of the configuration dialog are OK and Cancel buttons.

Configure Untrust Interface - Virtual Router

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

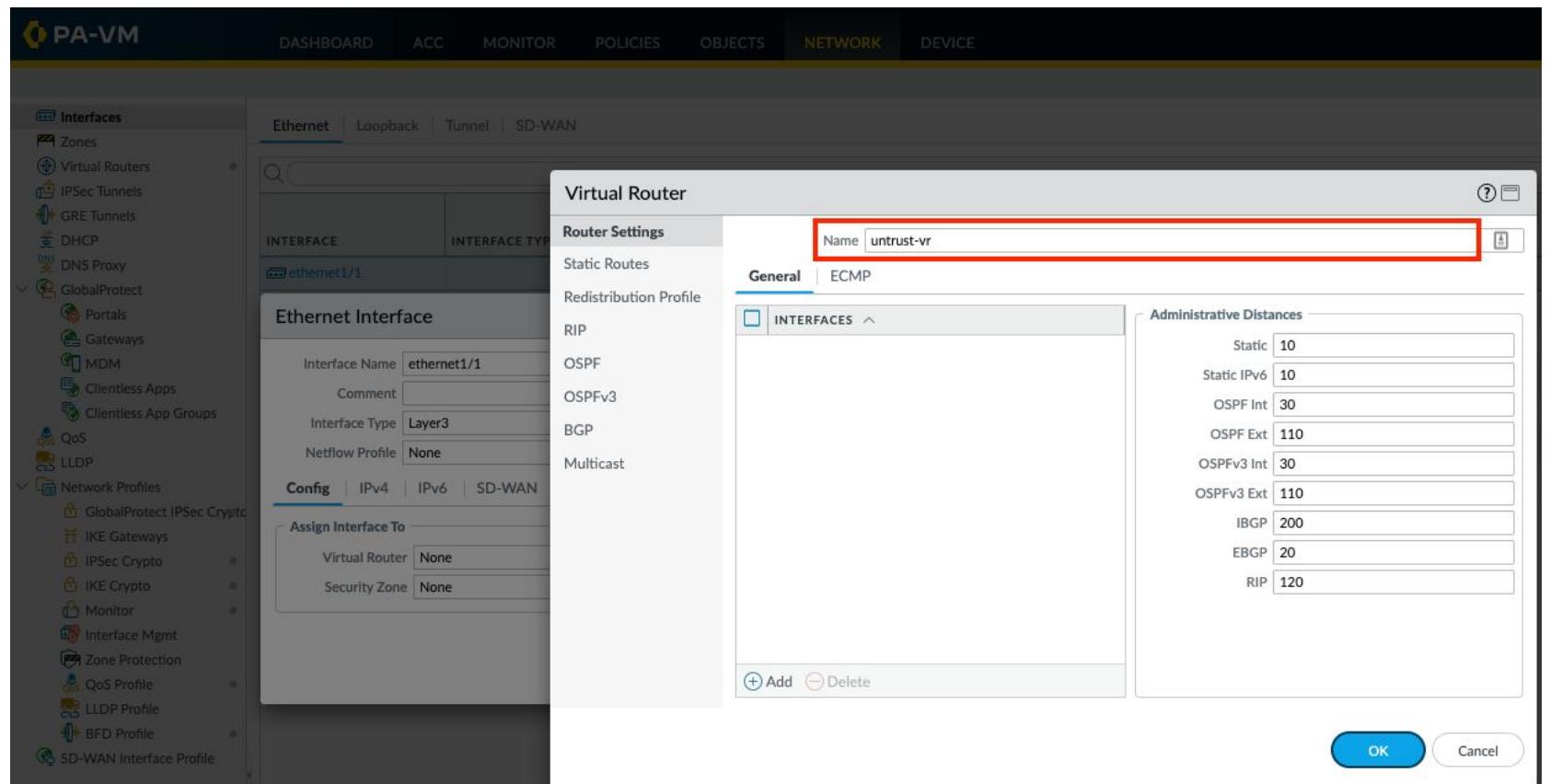
The screenshot shows the PA-VM interface with the following details:

- Top Navigation:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), DEVICE.
- Left Sidebar:** Interfaces (selected), Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (Portals, Gateways, MDM, Clientless Apps, Clientless App Groups), QoS, LLDP, Network Profiles (GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile).
- Ethernet Tab:** Ethernet, Loopback, Tunnel, SD-WAN.
- Ethernet Interface Table:**

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG
ethernet1/1				none	none	Untagged
- Ethernet Interface Configuration:**
 - Interface Name: ethernet1/1
 - Comment: (empty)
 - Interface Type: Layer3
 - Netflow Profile: None
- Assign Interface To:**
 - Virtual Router: None (selected)
 - Security Zone: None, default
 - New Virtual Router: (button)
- Buttons:** OK, Cancel.

Configure Untrust Interface - Virtual Router

- provide a proper name
- select “ok”



Configure Untrust Interface - Zone

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

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The left sidebar lists various network objects: Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (selected), Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, and L2TP Profiles.

The main pane shows the Ethernet interface configuration for "Ethernet | Loopback | Tunnel | SD-WAN". A table lists the interface "ethernet1/1" with columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, IP ADDRESS, VIRTUAL ROUTER, and TAG. The interface type is "Layer3" and the tag is "Untagged".

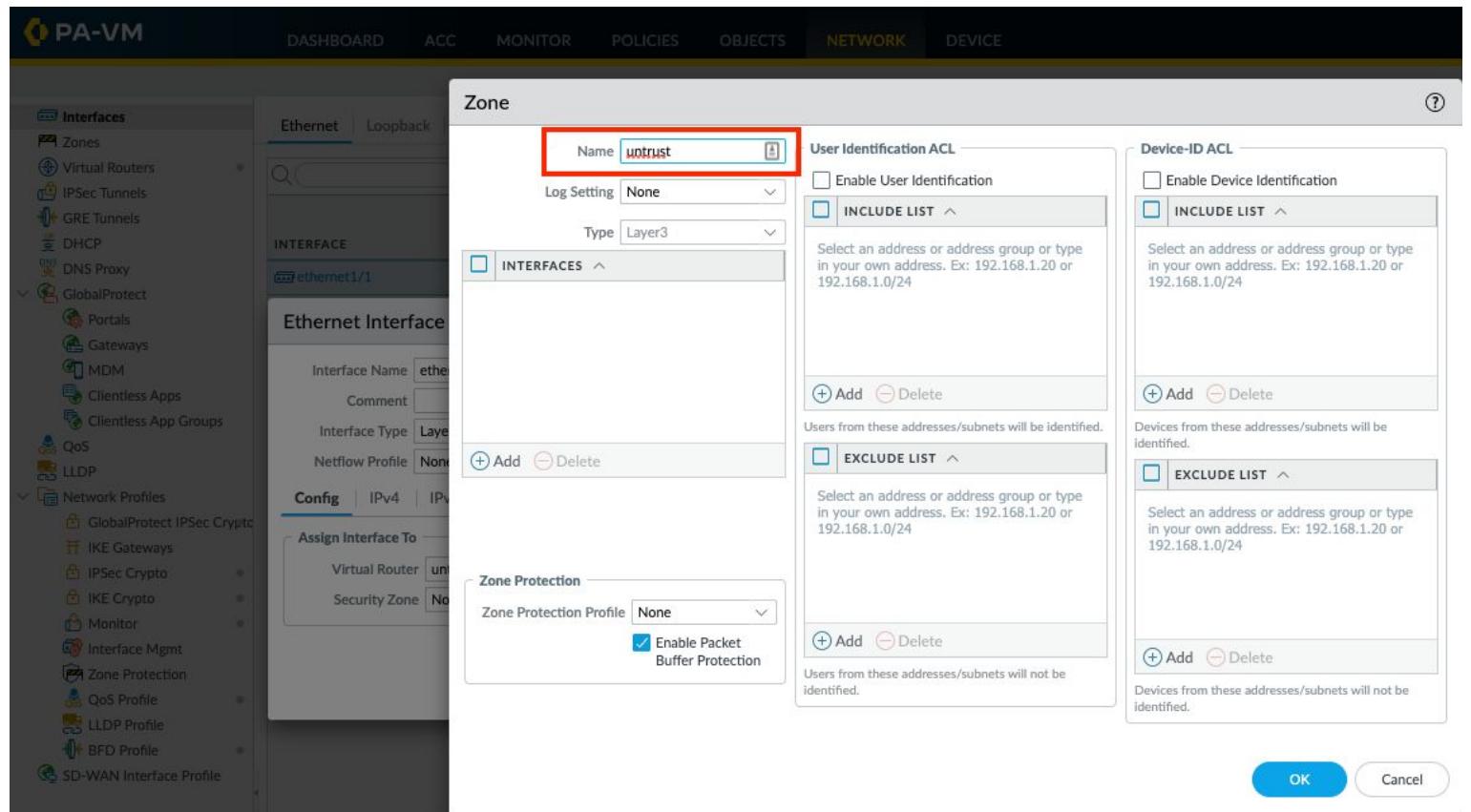
The "Ethernet Interface" configuration panel shows the following fields:

- Interface Name: ethernet1/1
- Comment: (empty)
- Interface Type: Layer3
- Netflow Profile: None

The "Config" tab is selected. The "Assign Interface To" section shows the "Virtual Router" set to "untrust-vr" and the "Security Zone" dropdown, which is highlighted with a red box. The dropdown menu lists "None" and "New [Zone]".

Configure Untrust Interface - Zone

- provide a proper name
- select “ok”



Configure Untrust Interface - Advanced

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

The screenshot shows the Palo Alto VM (PA-VM) interface configuration. The left sidebar lists various network components like Interfaces, Zones, Virtual Routers, and GlobalProtect. The main pane shows the 'Ethernet' tab selected under 'Interfaces'. A table lists the 'ethernet1/1' interface with details such as Interface Name, Interface Type (Layer3), Management Profile (None), Link State (Up), IP Address (none), Virtual Router (none), Tag (Untagged), and VLAN / Virtual Wire (none). A modal window titled 'Interface Management Profile' is open, allowing configuration of administrative management services and network services. In the 'Administrative Management Services' section, 'HTTP' and 'SSH' are checked. In the 'Network Services' section, 'Ping', 'HTTP OCSP', 'SNMP', 'Response Pages', 'User-ID', 'User-ID Syslog Listener-SSL', and 'User-ID Syslog Listener-UDP' are listed. A 'PERMITTED IP ADDRESSES' section contains the entry '168.63.129.16/32'. At the bottom right of the modal are 'OK' and 'Cancel' buttons.

Configure Trust Interface - Config

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

The screenshot shows the PA-VM interface with the following details:

Left Sidebar (Interfaces):

- Zones
- Virtual Routers
- IPSec Tunnels
- GRE Tunnels
- DHCP
- DNS Proxy
- GlobalProtect (selected)
- Portals
- Gateways
- MDM
- Clientless Apps
- Clientless App Groups
- QoS
- LLDP
- Network Profiles (selected)
- GlobalProtect IPSec Crypto
- IKE Gateways
- IPSec Crypto
- IKE Crypto
- Monitor
- Interface Mgmt
- Zone Protection
- QoS Profile
- LLDP Profile
- BFD Profile

Top Navigation Bar:

- DASHBOARD
- ACC
- MONITOR
- POLICIES
- OBJECTS
- NETWORK** (selected)
- DEVICE

Ethernet Interface Configuration:

Ethernet Tab: Shows a table of interfaces:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged
ethernet1/2			Up	None	None	Untagged

Ethernet Interface Dialog:

Interface Name: **ethernet1/2**
Comment:
Interface Type: **Layer3**
Netflow Profile: **None**

Config Tab: Selected. Other tabs include IPv4, IPv6, SD-WAN, Advanced.

Assign Interface To:

Virtual Router: **None**
Security Zone: **None**

Buttons: OK, Cancel

Configure Trust Interface - IPv4

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

The screenshot shows the PA-VM interface with the following details:

Network Tab: The **NETWORK** tab is selected.

Interfaces List: The **Ethernet** tab is selected in the list. The table shows two entries:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged
ethernet1/2			Up	none	none	Untagged

Ethernet Interface Configuration: The **Ethernet Interface** dialog is open for the **ethernet1/2** interface.

General: Interface Name: **ethernet1/2**, Comment: [empty], Interface Type: **Layer3**, Netflow Profile: **None**.

IPv4: Selected tab. Options include: Enable SD-WAN, Type: Static, PPPoE, DHCP Client, Enable, Automatically create default route pointing to default gateway provided by server, Send Hostname: **system-hostname**, Default Route Metric: **10**.

Buttons: OK, Cancel.

Configure Trust Interface - Virtual Router

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

The screenshot shows the Palo Alto VM (PA-VM) interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The left sidebar lists various network components: Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect (selected), Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles (GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, SD-WAN Interface Profile). The main pane displays the 'Ethernet' tab under the 'Interfaces' section, showing two interfaces: ethernet1/1 (Layer3, Management Profile: allow-health-probe, IP Address: Dynamic-DHCP Client, Virtual Router: untrust-vr, Tag: Untagged, VLAN/Virtual-Wire: none, Security Zone: untrust) and ethernet1/2 (Layer3, Management Profile: none, IP Address: none, Virtual Router: none, Tag: Untagged, VLAN/Virtual-Wire: none, Security Zone: none). A modal window titled 'Ethernet Interface' is open for ethernet1/2. It shows the 'Interface Name' as 'ethernet1/2', 'Comment' as ' ', 'Interface Type' as 'Layer3', and 'Netflow Profile' as 'None'. The 'Config' tab is selected, showing 'Assign Interface To' options: 'Virtual Router' set to 'None', and 'Security Zone' set to 'None'. The 'Virtual Router' section contains a 'Router Settings' table with a row for 'Name' set to 'trust-vr', highlighted with a red box. Other tabs in the modal include 'General' (selected) and 'ECMP'. On the right side of the modal, there is a 'INTERFACES' section with an 'Add' button and a 'Delete' button, and an 'Administrative Distances' table with entries for Static (10), Static IPv6 (10), OSPF Int (30), OSPF Ext (110), OSPFv3 Int (30), OSPFv3 Ext (110), IBGP (200), EBGP (20), and RIP (120). At the bottom of the modal are 'OK' and 'Cancel' buttons.

Configure Trust Interface - Zone

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

The screenshot shows the PA-VM interface with the following details:

- Left Sidebar:** Shows various network components: Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, and Network Profiles.
- Top Navigation:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (highlighted), DEVICE.
- Ethernet Tab:** Shows a table of interfaces:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged
ethernet1/2			Up	none	none	Untagged
- Ethernet Interface Dialog:** Shows configuration for ethernet1/2:
 - Interface Name: ethernet1/2
 - Comment: (empty)
 - Interface Type: Layer3
 - Netflow Profile: None
 - Config Tab (selected): IP4, IP6, SD-WAN, Advanced
 - Assign Interface To:
 - Virtual Router: trust-vr
 - Security Zone: None (highlighted with a red box)
 - Options: None, untrust, New Zone

Configure Trust Interface - Zone

- provide a proper name
- select “ok”

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The NETWORK tab is selected, and the sub-tab Ethernet is also selected. On the left sidebar, under the ZONES section, the 'trust' zone is highlighted. The main pane displays a table of interfaces:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged	none	untrust
ethernet1/2			Up	none	none	Untagged	none	none

A modal dialog titled "Zone" is open for the "trust" zone. It contains the following fields:

- Interface Name: trust
- Comment: (empty)
- Interface Type: Layer3
- Netflow Profile: None
- Log Setting: None
- Type: Layer3
- Assign Interface To:
 - Virtual Router: (empty)
 - Security Zone: (empty)
- INTERFACES (checkbox):
 - + Add
 - Delete
- User Identification ACL:
 - Enable User Identification:
 - INCLUDE LIST (checkbox):
 - + Add
 - Delete
 - Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
- Device-ID ACL:
 - Enable Device Identification:
 - INCLUDE LIST (checkbox):
 - + Add
 - Delete
 - Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
- EXCLUDE LIST (checkbox):
 - + Add
 - Delete
- Zone Protection:
 - Zone Protection Profile: None
 - Enable Packet Buffer Protection

At the bottom right of the modal are "OK" and "Cancel" buttons.

Configure Trust Interface - Advanced

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

The screenshot shows the PA-VM interface configuration screen. The left sidebar has a tree view with 'Interfaces' selected, showing options like Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS, GlobalProtect (selected), Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, BFD Profile, and SD-WAN Interface Profile.

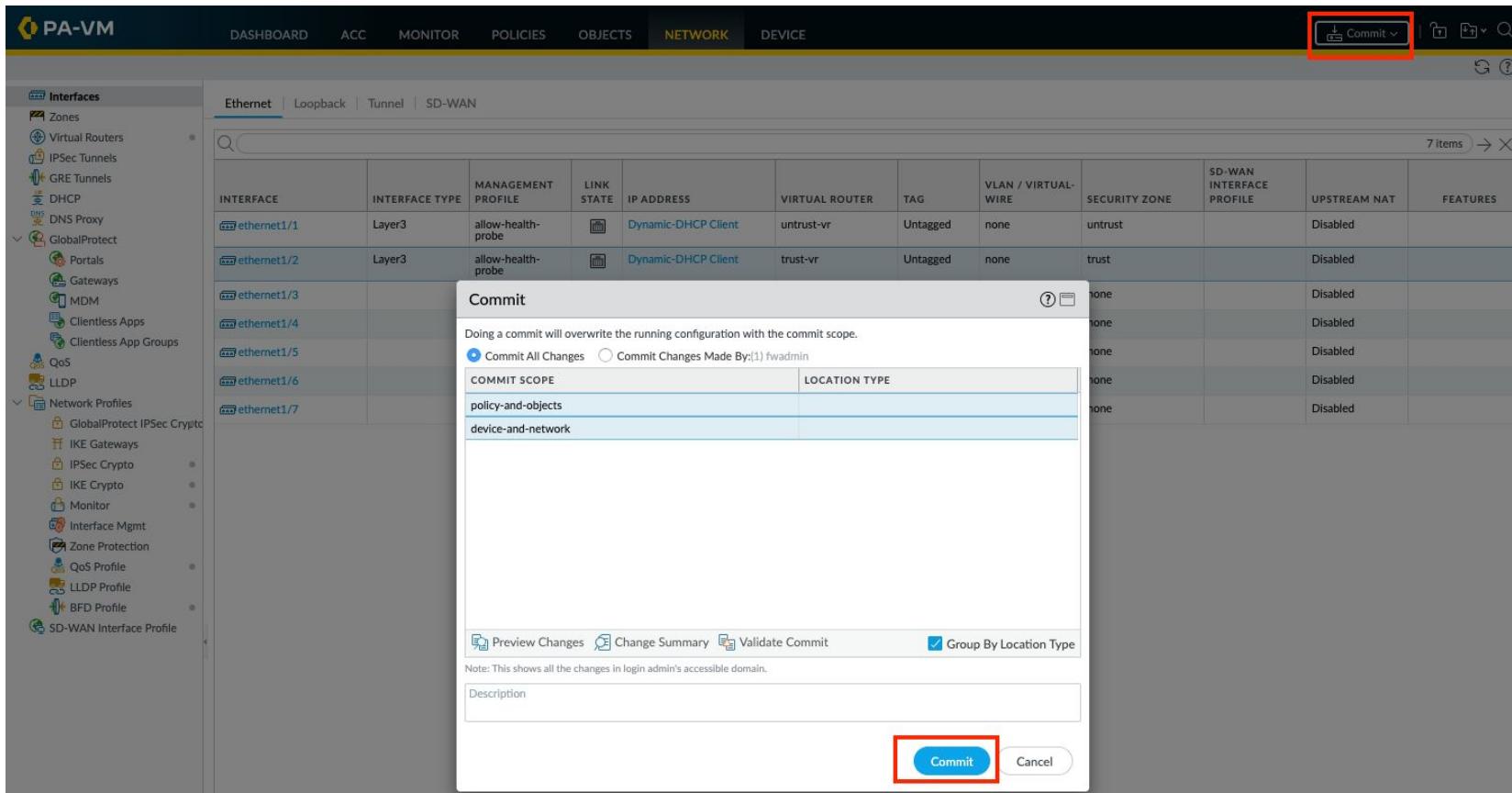
The main pane shows a table of Ethernet interfaces:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged
ethernet1/2	Layer3		Up	Dynamic-DHCP Client	trust-vr	Untagged

The 'ethernet1/2' row is selected, and its configuration details are shown in the bottom pane. The 'Advanced' tab is selected. The 'Management Profile' dropdown is set to 'None'. A red box highlights the 'Adjust TCP MSS' section, which contains a checkbox labeled 'allow-health-probe' and a 'New Management Profile' button. The 'OK' and 'Cancel' buttons are at the bottom right.

Commit your changes

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



Validate

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

The screenshot shows the Palo Alto Networks PA-VM interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (which is highlighted in yellow), and DEVICE. On the far right of the header are buttons for Commit, Undo, Redo, and Help.

The left sidebar contains icons for various network components: Interfaces (selected), Zones, Virtual Routers, IPSec Tunnels, GRE Tunnels, DHCP, DNS, DNS Proxy, GlobalProtect, Portals, and Content.

The main content area displays the 'Ethernet' tab under the 'Interfaces' section. A search bar at the top right shows '7 items'. The table lists two Ethernet interfaces:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES
ethernet1/1	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	untrust-vr	Untagged	none	untrust		Disabled	
ethernet1/2	Layer3	allow-health-probe	Up	Dynamic-DHCP Client	trust-vr	Untagged	none	trust		Disabled	

Repeat these steps on FW2 using the
same settings

Configure VM-Series

Routing on Virtual Routers

Configure Untrust Virtual Router

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

The screenshot shows the PA-VM interface with the following details:

- Left Sidebar:** Includes icons for Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, GRE Tunnels, DHCP, DNS, GlobalProtect (expanded), Portals, Gateways, MDM, Clientless Apps, and Clientless App Groups.
- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), DEVICE.
- Table View:** Shows a list of Virtual Routers. The row for "untrust-vr" is selected, showing its configuration: Name: untrust-vr, Interfaces: ethernet1/1, Configuration: ECMP status: Disabled.
- Detail View:** A modal window titled "Virtual Router - untrust-vr" displays the "Router Settings" for "untrust-vr".
 - General Tab:** Shows the Name field set to "untrust-vr".
 - ECMP Tab:** Shows the ECMP status as "Disabled".
 - Static Routes Tab:** Shows the "INTERFACES" dropdown with "ethernet1/1" selected.
 - RIP Tab:** Shows the RIP configuration.
 - OSPF Tab:** Shows the OSPF configuration.
 - Administrative Distances:** Shows Static AD as 10 and Static IPv6 AD as 10.

Configure Untrust Virtual Router

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

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

The screenshot shows the Palo Alto VM (PA-VM) interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), and DEVICE. The left sidebar lists various network components: Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPSec Crypto, and IKE Gateways. The main content area displays the 'Virtual Router - untrust-vr' configuration. Under 'Router Settings', the 'Static Routes' tab is selected, showing an IPv4 table with three entries:

NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
			TYPE	VALUE				
spoke-vnet	10.212.1.0/24		next-vr	trust-vr	default	10	None	unicast
default	0.0.0.0/0	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast
AZ-HealthProbe	168.63.129.16/32	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast

Configure Trust Virtual Router

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

The screenshot shows the PA-VM interface with the 'NETWORK' tab selected. In the left sidebar, under 'Virtual Routers', the 'trust-vr' router is selected. The main pane displays the 'Virtual Router - trust-vr' configuration. The 'Router Settings' section shows the name 'trust-vr'. Under 'General', the 'INTERFACES' dropdown is set to 'ethernet1/2'. Under 'Administrative Distances', the 'Static' value is 10 and the 'Static IPv6' value is 10. Other tabs like 'Static Routes', 'Redistribution Profile', 'RIP', 'OSPF', and 'OSPFv3' are also visible.

NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3	BGP
default		ECMP status: Disabled				
untrust-vr	ethernet1/1	Static Routes: 3 ECMP status: Disabled				
trust-vr	ethernet1/2	ECMP status: Disabled				

Configure Trust Virtual Router

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

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

The screenshot shows the Palo Alto Network Management interface (PA-VM) with the following details:

Top Navigation Bar: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (selected), DEVICE.

Left Sidebar: Interfaces, Zones, Virtual Routers (selected), IPSec Tunnels, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto.

Virtual Router - trust-vr:

- Router Settings:** IPv4 tab selected.
- Static Routes:** A table showing three static routes:

NAME	DESTINATION	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
spoke-vnet	10.212.1.0/24	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
internet	0.0.0.0/0		next-vr	untrust-vr	default	10	None	unicast
AZ-HealthProbe	168.63.129.16/32	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast

Palo Alto Networks Logo: paloalto NETWORKS

COMMIT YOUR CHANGES

Repeat these steps on FW2 using the
same settings

Configure VM-Series

NAT & Security Policies

Security Policies

Create Security Rules

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

The screenshot shows the Palo Alto VM interface. The top navigation bar has tabs: DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a yellow box), OBJECTS, NETWORK, and DEVICE. On the left, a sidebar menu is open under the “Security” section, which is also highlighted with a red box. The main content area displays a table of security policies. The table has columns for NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, and Destination (ZONE, ADDRESS, DEVICE). It also includes columns for APPLICATION, SERVICE, ACTION, PROFILE, and OPTIONS. Two policies are listed:

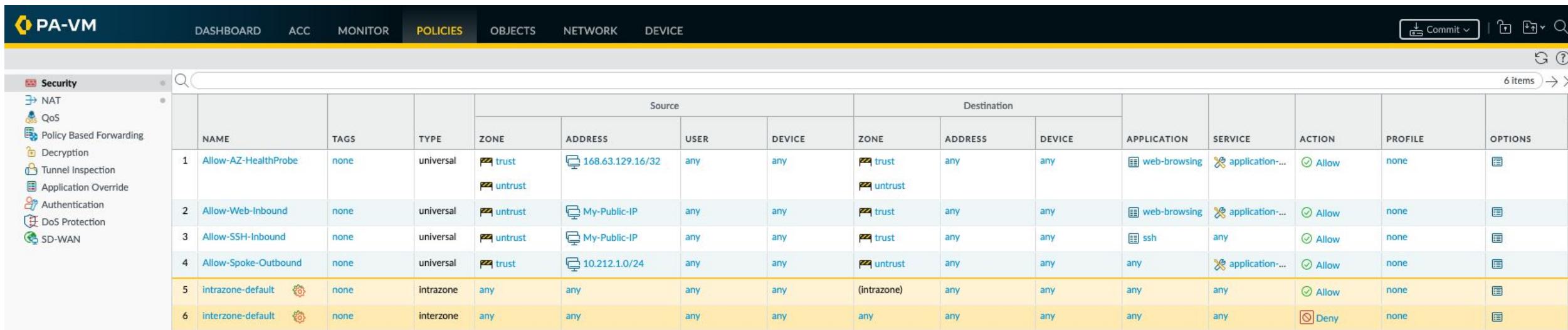
NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	none
2 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	none

Create Security Rules

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

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

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



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

COMMIT YOUR CHANGES

NAT Policies

Create NAT Policies

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

The screenshot shows the PA-VM (Palo Alto Virtual Machine) interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), OBJECTS, NETWORK, and DEVICE. On the far right of the header are buttons for Commit, Undo, Redo, and Search. The left sidebar contains a tree view of security policies: Security (selected), NAT (highlighted with a red box), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main content area displays a table for NAT policies. The table has three sections: "Original Packet" (with columns for NAME, TAGS, SOURCE ZONE, DESTINATION ZONE, DESTINATION INTERFACE, SOURCE ADDRESS, DESTINATION ADDRESS, and SERVICE), "Translated Packet" (with columns for SOURCE TRANSLATION and DESTINATION TRANSLATION), and "Rule Usage" (with columns for HIT COUNT, LAST HIT, and FIREWALL). A search bar at the top of the table area shows "0 items".

Create NAT Rules

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

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

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

COMMIT YOUR CHANGES

Repeat these steps on FW2 using the
same settings

Configure WebApp Resource Group

Next Steps

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

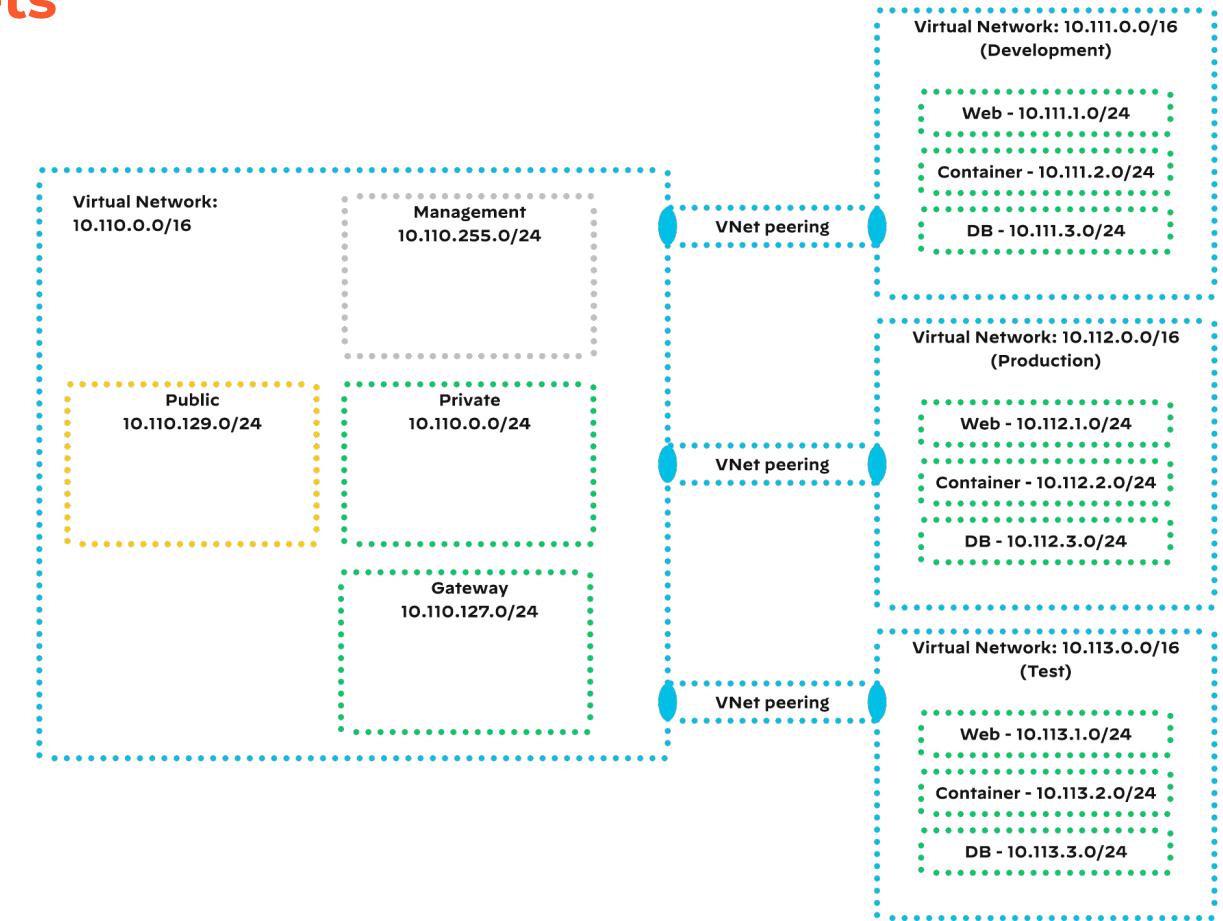
Configure WebApp Resource Group

Create VNet Peering

What is VNet Peering?

Full seamless IP reachability across VNets

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



Create VNET peering

- Select the Virtual Network in the Resource Group you created on [here](#)
 - Example “vnet-instructor”

The screenshot shows the Microsoft Azure portal interface for a resource group named "Pre-Req-Lab-Instructor". The "Overview" tab is selected. On the left, there's a sidebar with "Essentials" (Subscription, Deployment, Tags), "Resources" (Deployment, Security, Policies, Properties, Locks), and a search bar. The main area displays a table of resources with columns for Name, Type, Location, and three-dot ellipsis. The first resource listed is "vnet-instructor", which is highlighted with a red circle containing the number 1 and an arrow pointing to it.

Name	Type	Location	...
vnet-instructor	Virtual network	North Europe	...
vmseries-fw-vm1	Virtual machine	North Europe	...
vmseries-fw-vm2	Virtual machine	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

Add peering

vnet-instructor

This virtual network

Peering link name *

hub-to-spoke

1



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 or Route Server ⓘ

Use this virtual network's gateway or Route Server

Use the remote virtual network's gateway or Route Server

None (default)

Remote virtual network

Peering link name *

spoke-to-hub

2



Virtual network deployment model ⓘ

Resource manager

Classic

I know my resource ID ⓘ

Subscription *

AzureGCSPS

3



Virtual network *

spoke-vnet

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 or Route Server ⓘ

Use this virtual network's gateway or Route Server

Use the remote virtual network's gateway or Route Server

None (default)

4



Add

Create VNET peering

1. Use the same name
2. Use the same name
3. Select here the VNET that you created on
[Slide 16](#)
4. Select Add

Validate VNET peering

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information. Below the navigation bar, the breadcrumb trail shows the current location: Home > Microsoft.Template-20220613112504 > Pre-Req-Lab-Instructor > vnet-instructor. The main content area is titled "vnet-instructor | Peerings" and is described as a "Virtual network". On the left, there is a sidebar with links for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main pane displays a table of peerings. The table has columns for Name, Peering status, Peer, and Gateway transit. One entry is visible: "hub-to-spoke" with Peering status "Connected", Peer "spoke-vnet", and Gateway transit "Disabled". There are also filter and sorting options at the top of the table.

Name	Peering status	Peer	Gateway transit
hub-to-spoke	Connected	spoke-vnet	Disabled

Configure WebApp Resource Group

Create/Configure Route Table

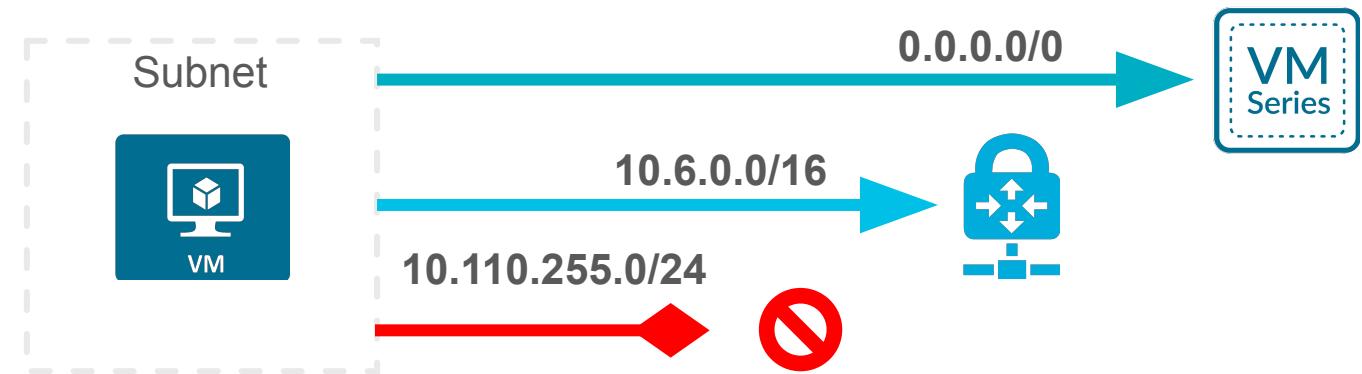
What is a Route Table/User defined Route?

Modify the default traffic forwarding behavior of Azure networking

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

The next-hop for the route can be

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



Create Route table

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and various icons. Below the navigation bar, the current resource group is displayed: 'Pre-Req-Instructor-WebApp' (Resource group). A red box highlights the 'Create' button in the top navigation bar. The main content area shows the 'Overview' tab selected under the 'Essentials' section. It displays basic information: Subscription (move) : A, Deployments : 1 Succeeded, Subscription ID : d, Location : North Europe, and Tags (edit) : Click here to add tags. On the left, a sidebar lists other tabs like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, and Events. At the bottom, there are filters for 'Type == all' and 'Location == all', and buttons for 'Add filter', 'No grouping', and 'List view'.

Create Route table

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

The screenshot shows the Microsoft Azure Marketplace interface. The search bar at the top contains the text "Route Table", which is highlighted with a red box. Below the search bar, there are several filter options: Pricing : All, Operating System : All, Publisher Type : All, Product Type : All, and Publisher name : All. A message indicates "No results were found." In the main search results area, three items are listed under "Showing results for 'Route Table'". The first item, "Route table" by Microsoft, is highlighted with a red box and has a red arrow pointing to it from the "Networking (2)" category in the sidebar. The second item is "VNS3 NATe - NAT Gateway Appliance" by Cohesive Networks. The third item is "Laravel" by Niles Partners Inc. Each result card includes a "Create" button at the bottom.

Create Web-App Route table

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

The screenshot shows the 'Create Route table' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. The 'Project details' section includes fields for 'Subscription' (set to 'AzureGCSPS'), 'Resource group' (set to 'Pre-Req-Instructor-WebApp'), and 'Create new'. The 'Instance details' section includes fields for 'Region' (set to 'North Europe') and 'Name' (set to 'webapp-rt'). A 'Propagate gateway routes' checkbox is checked ('Yes'). Step 1 is highlighted with a red circle and arrow pointing to the 'Subscription' field. Step 2 and 3 are highlighted with a red circle and arrows pointing to the 'Region' and 'Name' fields respectively. Step 4 is highlighted with a red circle and arrow pointing to the 'Review + create' button at the bottom.

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 * ① Resource group * ①

AzureGCSPS
Pre-Req-Instructor-WebApp
Create new

Instance details

Region * ① Name * ① Propagate gateway routes * ①

North Europe
webapp-rt
Yes
No

Review + create < Previous Next : Tags >

Create Web-App Route table

1. Select Create after the validation passed

The screenshot shows the Microsoft Azure portal interface for creating a route table. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Pre-Req-Instructor-WebApp > Create a resource > Marketplace > Create Route table'. A green banner at the top right indicates 'Validation Passed'. Below this, there are tabs for 'Basics', 'Tags', and 'Review + create' (which is underlined, indicating it's the active step). On the left, there's a 'TERMS' section with a detailed legal agreement. On the right, the 'Basics' section displays the following configuration:

Subscription	AzureGCSPS
Resource group	Pre-Req-Instructor-WebApp
Region	North Europe
Name	webapp-rt
Propagate gateway routes	Yes

At the bottom, there's a navigation bar with a red circle containing the number '1' and an orange arrow pointing to a blue 'Create' button. Other buttons include '< Previous', 'Next', and 'Download a template for automation'.

Configure Route Table

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

The screenshot shows the Microsoft Azure Resource Group Overview page for the 'Pre-Req-Instructor-WebApp' resource group. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The left sidebar lists various settings like Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, Policies, Properties, Locks, and Cost Management. The main content area displays the 'Essentials' section with details such as Subscription (move) to 'AzureGCSPS', Subscription ID 'd47f1af8-9795-4e86-bbce-da72cf0f8ec', Tags, and Deployments. Below this is a 'Resources' section with a table listing seven records. A red arrow points to the 'webapp-rt' entry in the table, which is a Route table located in North Europe.

Name	Type	Location	Actions
simple-vm_OsDisk_1_5d44c5387db04af5858f85bc401fc1ae	Disk	North Europe	...
default-NSG	Network security group	North Europe	...
myVMNic	Regular Network Interface	North Europe	...
webapp-rt	Route table	North Europe	...

Associate Route table with a subnet

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

The screenshot shows the Microsoft Azure portal interface for managing a Route Table named 'webapp-rt'. The left sidebar has a 'Subnets' item highlighted with a red circle containing '1'. A red arrow points from this circle to the 'Associate' button in the top navigation bar, which is also highlighted with a red circle containing '2'. The main content area displays a table with columns: Name, Address range, Virtual network, and Security group. A search bar at the top of the table says 'Search subnets'.

Microsoft Azure

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

Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt

webapp-rt | Subnets

Route table

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Properties

Associate

Search subnets

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓
No results.			

Associate Route table with a subnet

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

The screenshot shows the Microsoft Azure portal interface for managing a Route Table named 'webapp-rt'. The left sidebar has a 'Subnets' item highlighted with a red circle labeled '1'. The main content area shows a search bar for subnets with a red circle labeled '2' and a 'Associate' button. Below the search bar is a table with columns: Name, Address range, Virtual network, and Security group. A message says 'No results.'

Microsoft Azure

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

Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt

webapp-rt | Subnets

Route table

Search (Cmd+ /) 2 Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets 1

Properties

Search subnets

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓
No results.			

Associate Route table with a subnet

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. Below the navigation bar, the URL path is visible: Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), and Tags. The main content area shows a 'Subnets' section for the 'webapp-rt' route table. A 'Associate' button is highlighted with a red circle containing the number '2'. A large orange arrow points from this button to a modal dialog titled 'Associate subnet'. The dialog has a search bar with 'spoke-v' typed into it. Below the search bar is a dropdown menu listing three items: 'Pre-Req-Instructor-WebApp', 'spoke-vnet', and 'spoke-vnet'. The 'Pre-Req-Instructor-WebApp' item is currently selected.

Associate Route table with a subnet

- Validate that subnet is listed under “Subnets”

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (tostern@paloaltonetwo...). Below the navigation bar, the breadcrumb trail indicates the current location: Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt.

The main content area displays the "webapp-rt | Subnets" page. On the left, there is a sidebar with various navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Routes, and Subnets. The "Subnets" link is highlighted with a red box.

The main content area features a search bar labeled "Search subnets" and a table listing subnets. The columns are: Name, Address range, Virtual network, and Security group. One row in the table is highlighted with a red box, showing the following details:

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

Create static Route

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

The screenshot shows the Microsoft Azure portal interface for creating a static route. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (tostern@paloaltonetwo...). Below the navigation bar, the breadcrumb trail shows: Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt. The main content area is titled "webapp-rt | Routes" and shows a "Route table". On the left, a sidebar lists "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings", "Configuration", and "Routes". A red arrow labeled "1" points to the "Routes" link in the sidebar. At the top of the main content area, there is a search bar, a "Give feedback" button, and a "Add" button. A red arrow labeled "2" points to the "Add" button. The main table area has columns for "Name ↑↓", "Address prefix ↑↓", and "Next hop type ↑↓". A message at the bottom of the table says "No results."

Create static Route

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

The screenshot shows the Microsoft Azure portal interface for creating a static route. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information (tostern@paloaltonetwo...). Below the navigation bar, the breadcrumb trail shows the current location: Home > Microsoft.RouteTable-20220613115301 > Pre-Req-Instructor-WebApp > webapp-rt. The main content area is titled "webapp-rt | Routes" and shows a "Route table". On the left, a sidebar lists options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, and Routes (which is highlighted with a red arrow labeled "1"). At the top of the main content area, there is a search bar, a "Give feedback" button, and a "Add" button (which is highlighted with a red arrow labeled "2"). The main table displays columns for Name, Address prefix, and Next hop type, with a note stating "No results."

Create static Route

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

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

Add route

Route name * LB-route

Address prefix destination * IP Addresses

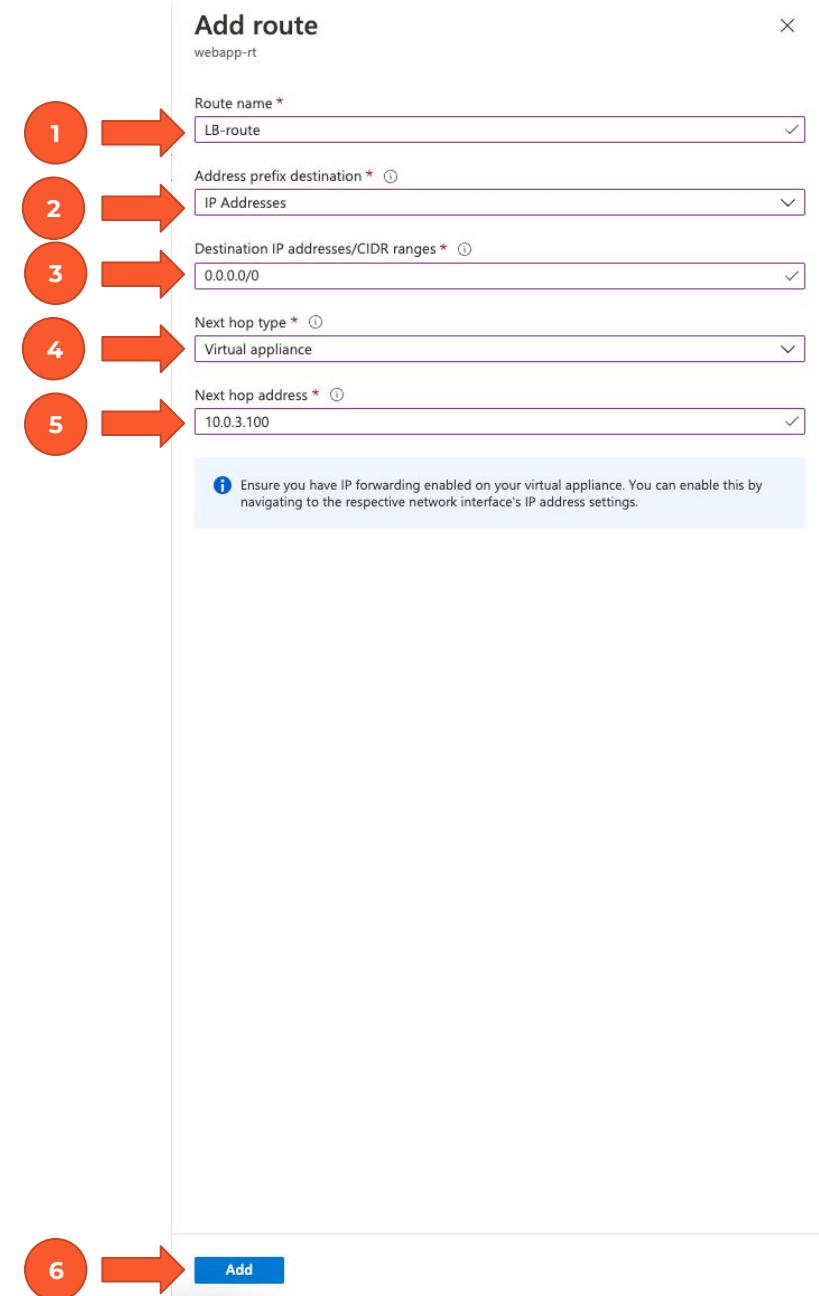
Destination IP addresses/CIDR ranges * 0.0.0.0/0

Next hop type * Virtual appliance

Next hop address * 10.0.3.100

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

6 → Add



Validate static Route

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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. The user's email, tostern@paloaltonetwo..., and the Palo Alto Networks Inc. (PA...) logo are visible on the right. The main content area displays the 'webapp-rt | Routes' page. On the left, a sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, and Routes. The 'Routes' option is currently selected and highlighted in grey. The main content area features a search bar labeled 'Search routes' and a table with three columns: 'Name' (sorted by address prefix), 'Address prefix', and 'Next hop type'. A single row is present in the table, showing 'LB-route' as the name, '0.0.0.0/0' as the address prefix, and 'VirtualAppliance' as the next hop type. There is also a '...' button at the end of the table row.

Name ↑↓	Address prefix ↑↓	Next hop type ↑↓
LB-route	0.0.0.0/0	VirtualAppliance

Configure Web Server

Configure Web Server

Login into Web Server

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

```
M-C02FG2PMMD6M:~ tostern$ ssh fwadmin@5 12
fwadmin@5          's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1083-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Jun 14 08:11:15 UTC 2022

System load: 0.0          Processes:      120
Usage of /: 7.0% of 28.90GB  Users logged in:  1
Memory usage: 34%          IP address for eth0: 10.212.1.4
Swap usage:  0%

2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jun 14 07:57:01 2022 from 34.99.221.241
fwadmin@simple-vm:~$
```

Update Web Server

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

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

Install Web Server

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

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

Test Traffic flow

Connect to Web Server

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



Validate Outbound Traffic in your logs

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

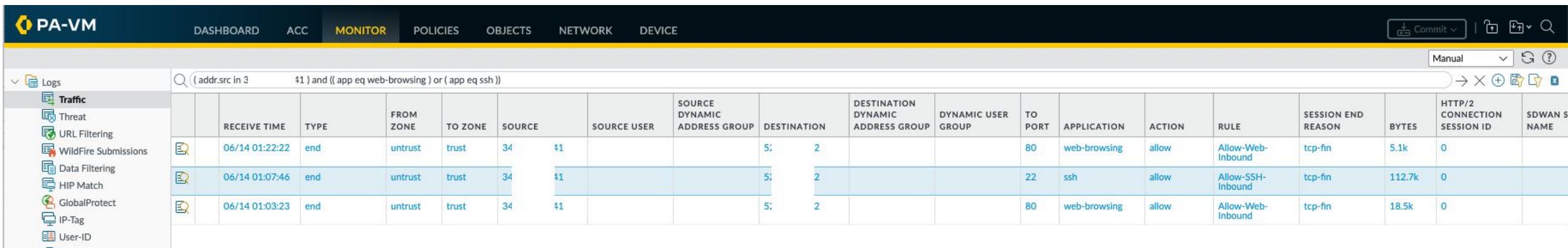


The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, a sidebar lists various log categories: Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, GlobalProtect, and IP-Tag. The 'Logs' category is expanded, and 'Traffic' is selected. A search bar at the top contains the filter: '(addr.src in 10.212.1.4) and (app eq apt-get)'. The main area displays a table of log entries:

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

Validate Inbound Traffic in your logs

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



The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left, a sidebar menu is open under the 'Logs' section, with 'Traffic' selected. The main area displays a table of log entries. The table has the following columns: RECEIVE TIME, TYPE, FROM ZONE, TO ZONE, SOURCE, SOURCE USER, SOURCE DYNAMIC ADDRESS GROUP, DESTINATION, DESTINATION DYNAMIC ADDRESS GROUP, DYNAMIC USER GROUP, TO PORT, APPLICATION, ACTION, RULE, SESSION END REASON, BYTES, HTTP/2 CONNECTION SESSION ID, and SDWAN S NAME. A search bar at the top of the table contains the filter: '(addr.src in 3.41) and ((app eq web-browsing) or (app eq ssh))'. Three log entries are shown:

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES	HTTP/2 CONNECTION SESSION ID	SDWAN S NAME
06/14 01:22:22	end	untrust	trust	34.41			5.2			80	web-browsing	allow	Allow-Web-Inbound	tcp-fin	5.1k	0	
06/14 01:07:46	end	untrust	trust	34.41			5.2			22	ssh	allow	Allow-SSH-Inbound	tcp-fin	112.7k	0	
06/14 01:03:23	end	untrust	trust	34.41			5.2			80	web-browsing	allow	Allow-Web-Inbound	tcp-fin	18.5k	0	

Change Web Server default page

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





Thank you



paloaltonetworks.com

Backup Slides

How to find Frontend IP addresses of Internal Load Balancer?

- Navigate to your resource group you created [here](#) and select the “vmseries-internal-lb”

The screenshot shows the Azure portal interface for a resource group named "Pre-Rq-Lab-Instructor". The left sidebar contains navigation links for Home, Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Deployments, Security, Policies, Properties, Locks, Cost Management, and Cost analysis. The "Overview" tab is selected.

The main content area displays the "Essentials" section with details about the subscription, deployments, location, and tags. It also shows a list of resources under the "Resources" tab, including "vmseries-fw-as", "vmseries-fw-vm1_OsDisk_1", "vmseries-fw-vm2_OsDisk_1", "vmseries-internal-lb", and "vmseries-public-lb". The "vmseries-internal-lb" resource is highlighted with a red box.

Name	Type	Location	Actions
vmseries-fw-as	Availability set	North Europe	...
vmseries-fw-vm1_OsDisk_1	Disk	North Europe	...
vmseries-fw-vm2_OsDisk_1	Disk	North Europe	...
vmseries-internal-lb	Load balancer	North Europe	...
vmseries-public-lb	Load balancer	North Europe	...

How to find Frontend IP addresses of Internal Load Balancer?

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

The screenshot shows the Microsoft Azure portal interface for managing a load balancer. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information. Below the navigation bar, the breadcrumb navigation shows: Home > Pre-Req-Lab-Instructor > vmseries-internal-lb. The main title is "vmseries-internal-lb | Frontend IP configuration". On the left, there is a sidebar with links for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The "Frontend IP configuration" link is highlighted with a red box. The main content area displays a table with the following data:

Name ↑↓	IP address ↑↓	Rules count ↑↓
LoadBalancerFrontEnd	10.0.3.100	1

A filter bar labeled "Filter by name..." is positioned above the table. The entire IP address "10.0.3.100" is also highlighted with a red box.

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

- Navigate to your resource group you created [here](#) and select the “vmseries-public-lb”

The screenshot shows the Microsoft Azure portal interface for a resource group named "Pre-Req-Lab-Instructor". The "Overview" tab is selected on the left sidebar. The main content area displays the "Essentials" section with subscription information and deployment status. Below this, the "Resources" section lists 21 records, including a public load balancer named "vmseries-public-lb" which is highlighted with a red box. The table shows columns for Name, Type, Availability set, Location, and three ellipsis buttons for each row.

Name	Type	Availability set	Location
vmseries-fw-as	Disk	North Europe	...
vmseries-fw-vm1_OsDisk_1_48695af59dc24256b961ce7ebb853d61	Disk	North Europe	...
vmseries-fw-vm2_OsDisk_1_daabf619a87c488c9254d1e0c82c4857	Disk	North Europe	...
vmseries-internal-lb	Load balancer	North Europe	...
vmseries-public-lb	Load balancer	North Europe	...

How to find Frontend IP addresses of Public Load Balancer?

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

The screenshot shows the Microsoft Azure portal interface for managing a load balancer. The top navigation bar includes the Microsoft Azure logo, a search bar, and user account information. Below the navigation, the URL indicates the resource is under 'Pre-Req-Lab-Instructor'. The main title is 'vmseries-public-lb | Frontend IP configuration'. On the left, a sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings (which is currently selected). Under Settings, 'Frontend IP configuration' is highlighted with a red box. The main content area displays a table with columns: Name, IP address, and Rules count. A single row is shown, named 'LoadBalancerFrontEnd' with an IP address of '52.12.12 (vmseries-public-lb-pip)'. The IP address column is also highlighted with a red box.

Name	IP address	Rules count
LoadBalancerFrontEnd	52.12.12 (vmseries-public-lb-pip)	4

How to find the IP addresses of my Web Server?

- Navigate to your resource group you created [here](#) and select the “simple-vm”

The screenshot shows the Microsoft Azure Resource Groups interface. The left sidebar lists categories like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Deployments, Security, Policies, Properties, Locks, and Cost Management. The main area displays the 'Pre-Req-Instructor-WebApp' resource group. The 'Overview' tab is selected. Key details shown include:

- Subscription (move) : A
- Subscription ID : d
- Tags (edit) : Click here to add tags
- Deployments : 2 Succeeded
- Location : North Europe

The 'Resources' section shows a list of 7 records:

Name	Type	Location	Actions
spoke-vnet	Virtual network	North Europe	...
simple-vm	Virtual machine	North Europe	...
bootdiags5lfo2ovieepw4	Storage account	North Europe	...
webapp-rt	Route table	North Europe	...
[redacted]	[redacted]	[redacted]	...
[redacted]	[redacted]	[redacted]	...

A red box highlights the 'simple-vm' row in the list.

How to find the IP addresses of my Web Server?

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