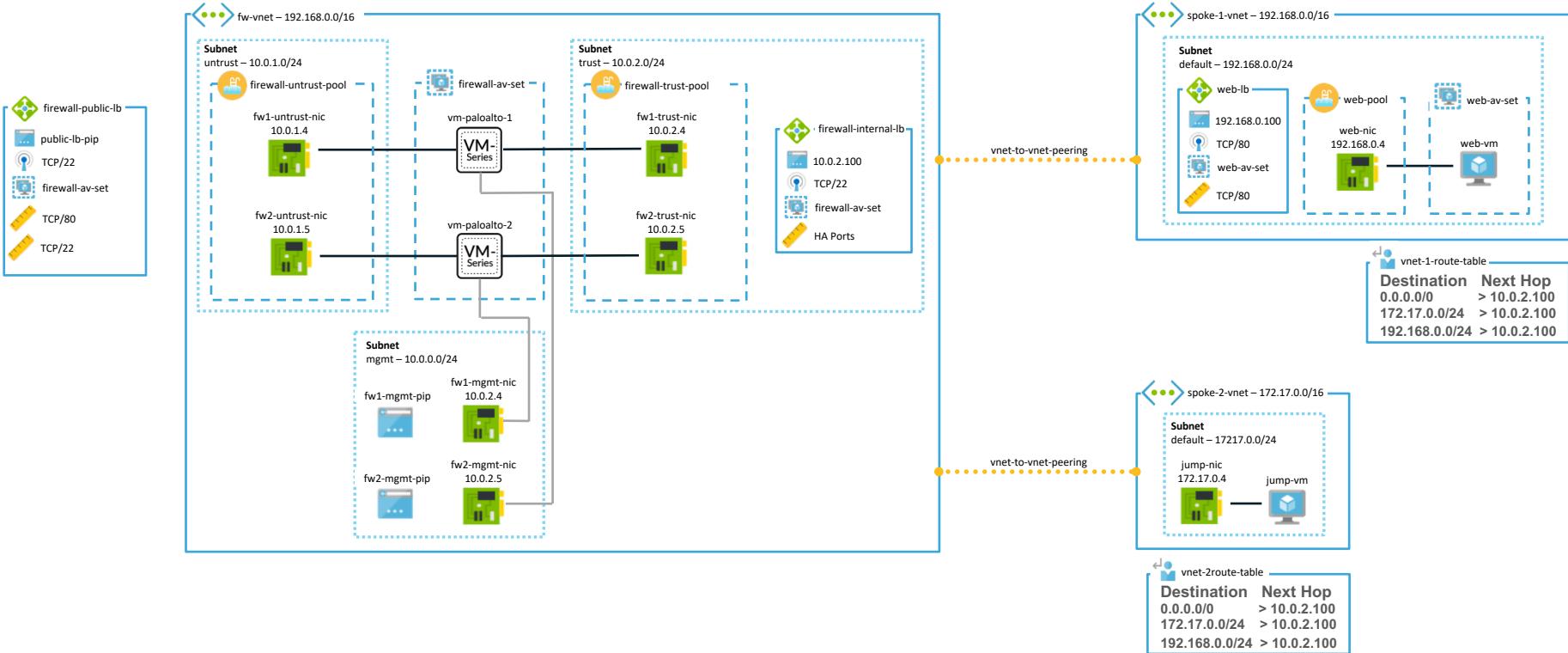


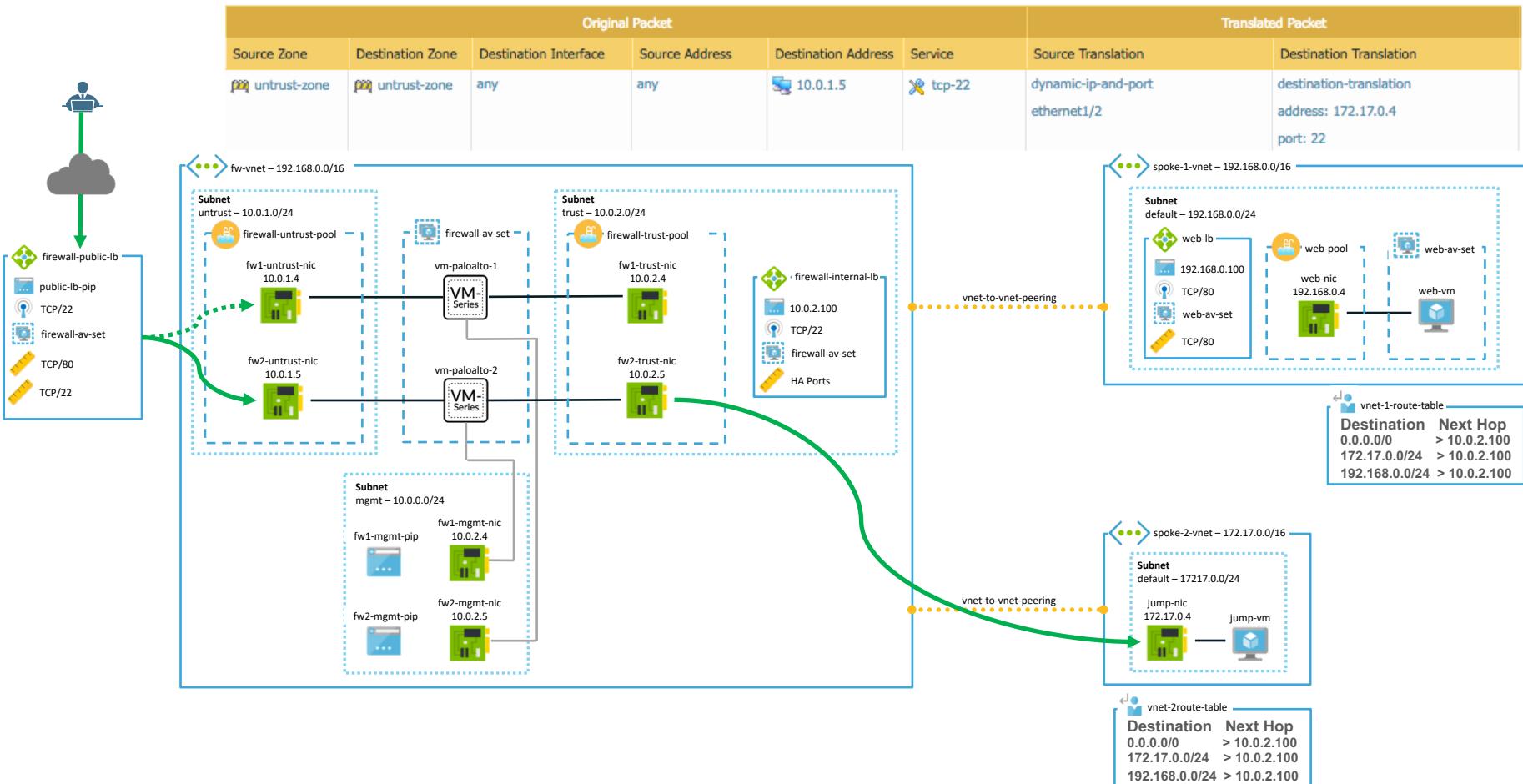
TRANSIT DEMO GUIDE

Matt McLimans, Public Cloud Consultant Engineer

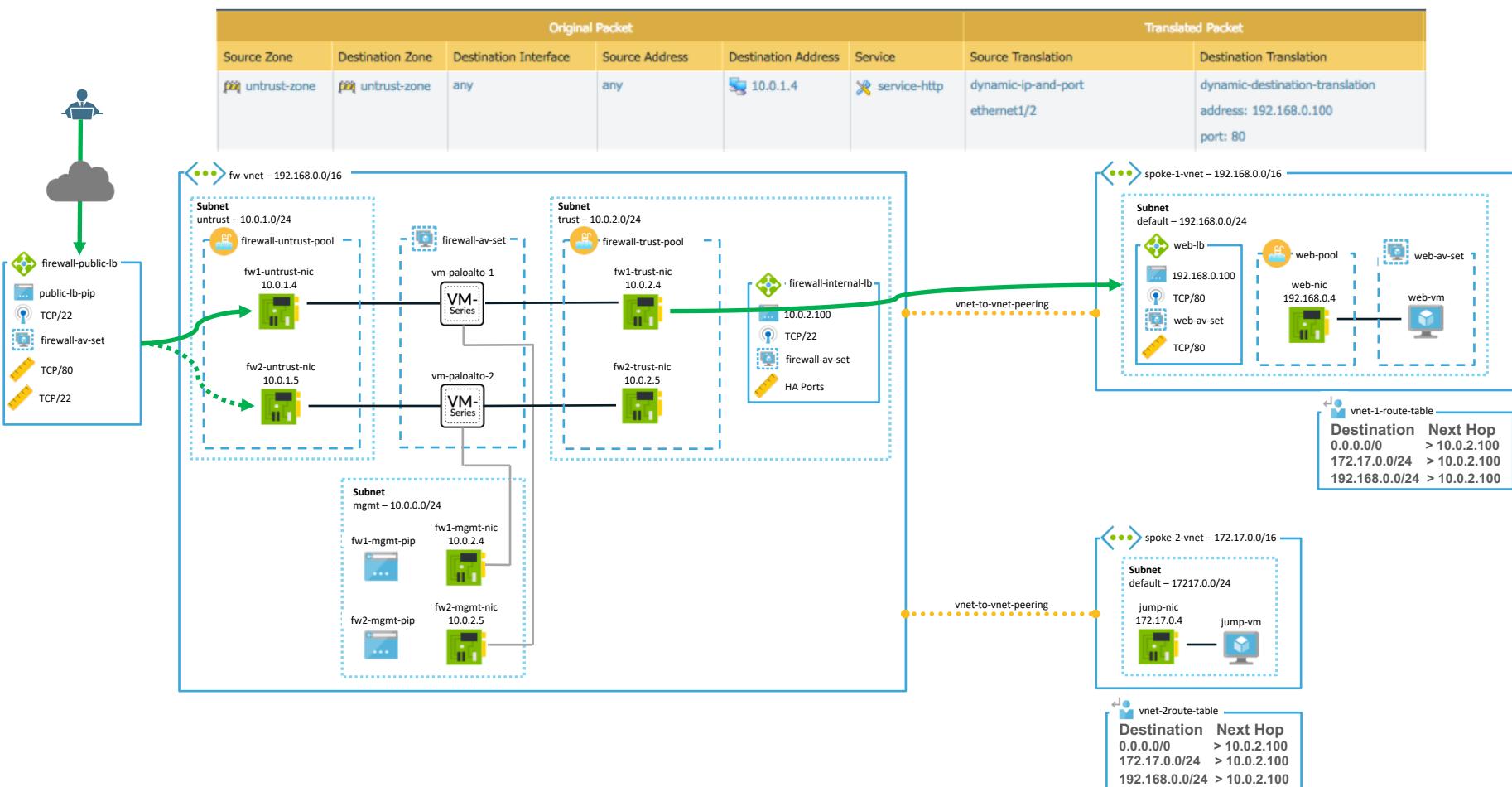




Environment Components

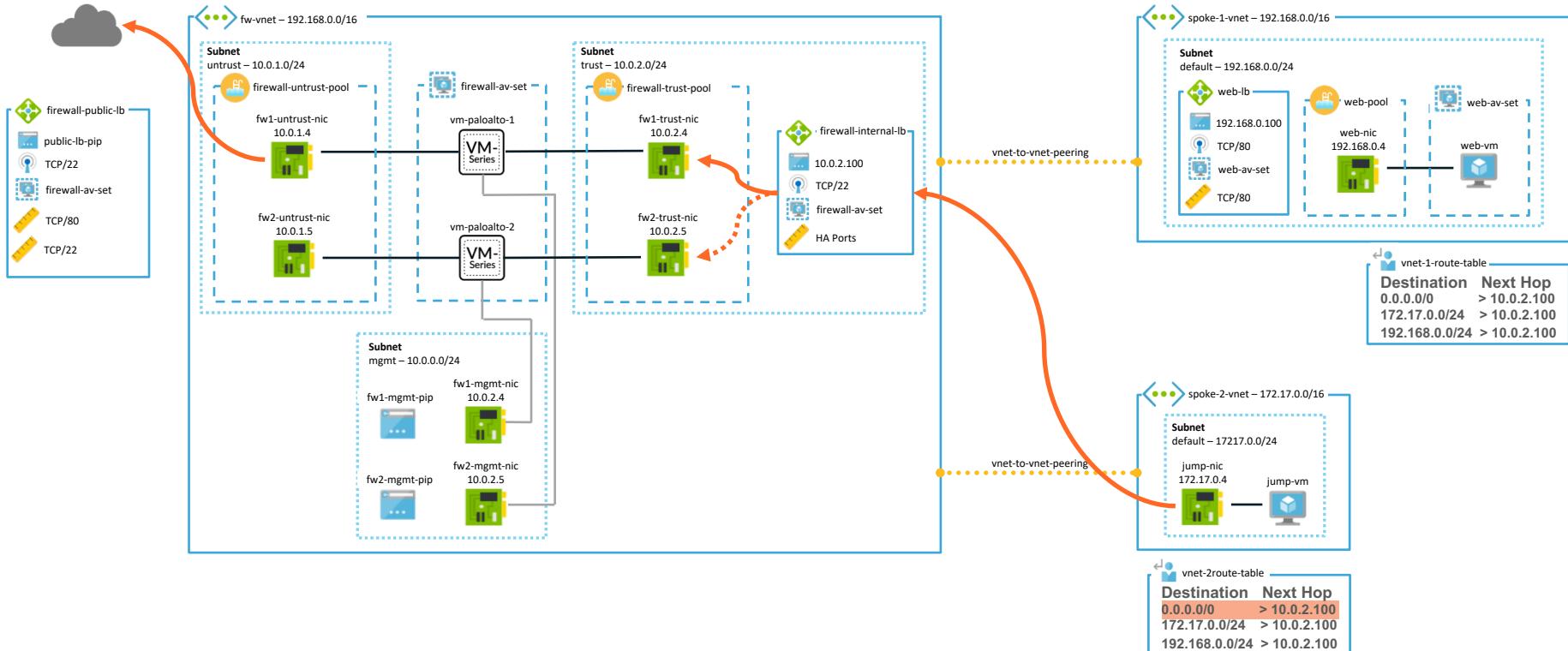


Inbound to Jump-VM in Spoke-2-VNET

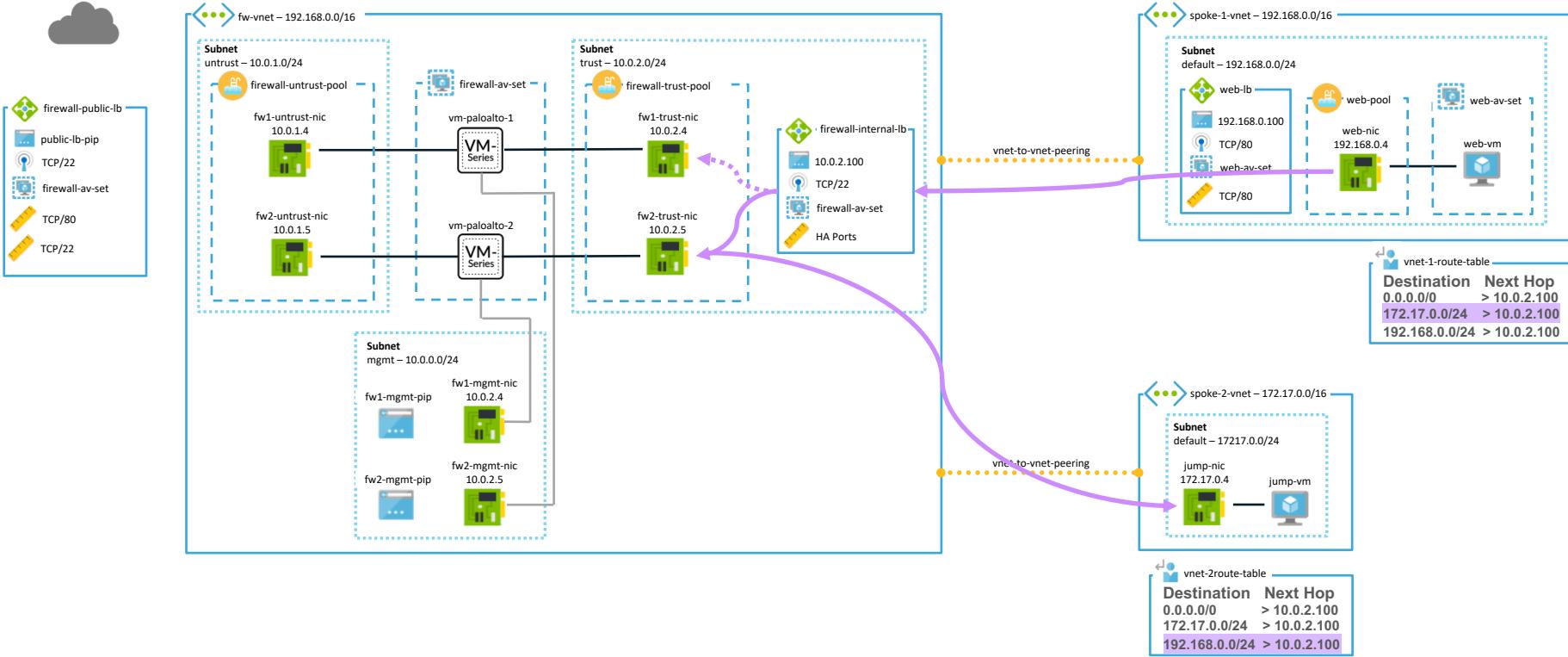


Inbound to Web LB in Spoke-1-VNET

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



Outbound from Spoke-2-VNET



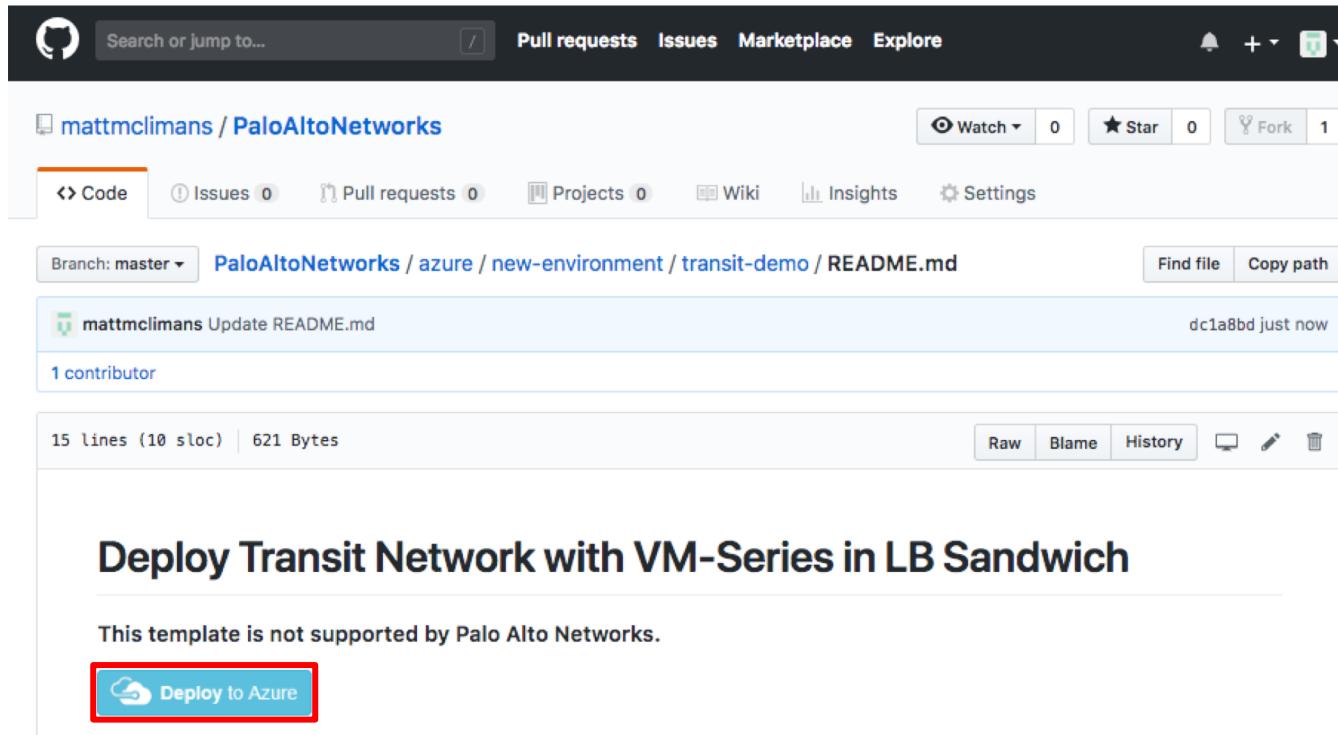
East-West between Spoke-1-VNET & Spoke-2-VNET



Deploy the Template

Step A1. Launch the Template

1. Go to:
https://github.com/wwce/azure-arm/tree/master/azure-arm-mclimans/demo_deployments/transit_2spokes_2fw_3nic_intlb_extlb
2. Click “Deploy to Azure”



The screenshot shows a GitHub repository page for `mattmclimans / PaloAltoNetworks`. The repository has 0 issues, 0 pull requests, 0 projects, and 1 contributor. The README.md file is displayed, showing a commit by `mattmclimans` that updated the README.md file just now. The file contains 15 lines (10 sloc) and 621 bytes. At the bottom of the README, there is a prominent blue button with white text that says "Deploy to Azure".

Branch: master ▾ [PaloAltoNetworks / azure / new-environment / transit-demo / README.md](#) [Find file](#) [Copy path](#)

 mattmclimans Update README.md dc1a8bd just now

1 contributor

15 lines (10 sloc) | 621 Bytes [Raw](#) [Blame](#) [History](#)

Deploy Transit Network with VM-Series in LB Sandwich

This template is not supported by Palo Alto Networks.

[!\[\]\(fa622bb7024fc0efe68a00f8b7fa72b4_img.jpg\) Deploy to Azure](#)



Step A2. Setup Auth Codes

1. Go to:

<https://support.paloaltonetworks.com>

The screenshot shows a GitHub repository page for 'mattmclimans / PaloAltoNetworks'. The repository has 0 issues, 0 pull requests, 0 projects, and 1 fork. The README.md file is displayed, showing a single commit by 'mattmclimans' that updated the README.md file just now. The file contains 15 lines (10 sloc) and 621 Bytes. At the bottom of the file content, there is a heading: 'Deploy Transit Network with VM-Series in LB Sandwich'. Below this heading, a message states: 'This template is not supported by Palo Alto Networks.' A blue button labeled 'Deploy to Azure' is present, with a red box drawn around it to indicate it as the target for Step A2.

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

2. Click "Deploy to Azure"



Step A3. Create New Resource Group

Custom deployment
Deploy from a custom template

TEMPLATE

 Customized template
28 resources

[Edit template](#) [Edit parameters](#) [Learn more](#)

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

BASICS

* Subscription: Visual Studio Professional

* Resource group: (New) palo-demo-group
[Create new](#)

* Location: East US

SETTINGS

* Username: paloalto

* Password: PanPassword123!



Step A4. Agree to Terms & Conditions

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

TERMS AND CONDITIONS

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party

I agree to the terms and conditions stated above

Purchase

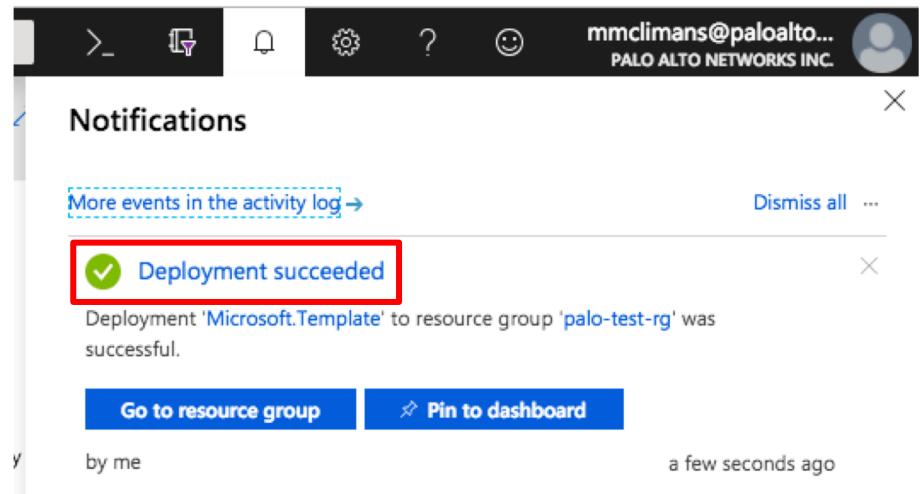
DO NOT CHANGE ANY OTHER FIELDS.



Step A5. Wait for deployment to complete...

Deployment takes ~10 Minutes to complete.

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





License the Firewall

Step B1. Find FW-1 Management IP.

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

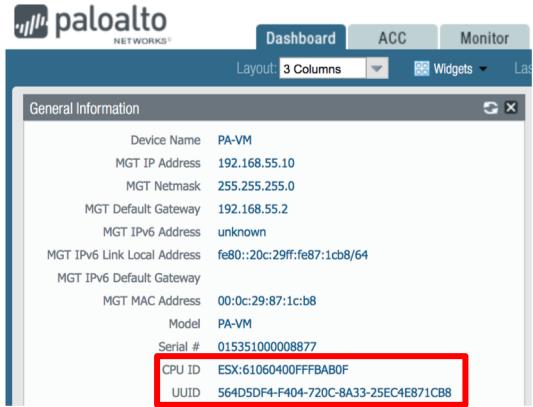
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with 'All resources' highlighted. In the center, the details for a Network Interface named 'fw1-mgmt-nic' are displayed. The 'Overview' tab is selected. Key information shown includes:

- Resource group: palo-test-rg
- Location: East US
- Subscription: Visual Studio Professional
- Private IP address: 10.0.0.4
- Virtual network/subnet: fw-vnet/mgmt
- Public IP address: 104.45.168.79 (fw1-mgmt-pip)

At the bottom of the Azure page, a browser window is open with the URL <https://104.45.168.79/php/login.php>. A red box highlights the URL bar and the public IP address. Below the browser, a Palo Alto Networks login screen is shown with the username 'paloalto' and password 'PanPassword123!' entered. A red box highlights the password field.

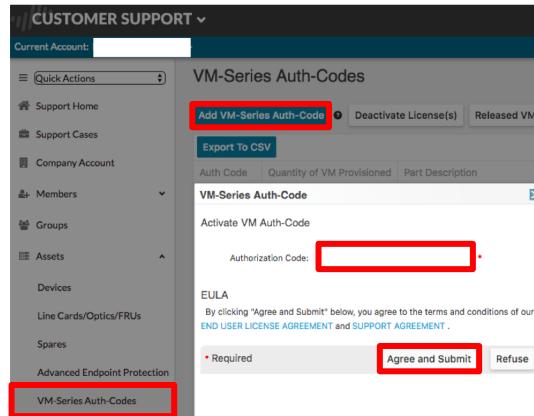
Step B2. License the VM-Series

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



Device Name PA-VM
MGT IP Address 192.168.55.10
MGT Netmask 255.255.255.0
MGT Default Gateway 192.168.55.2
MGT IPv6 Address unknown
MGT IPv6 Link Local Address fe80::20c:29ff:fe87:1cb8/64
MGT IPv6 Default Gateway
MGT MAC Address 00:0c:29:87:1c:b8
Model PA-VM
Serial # 015351000008877
CPU ID ESX:61060400FFFBAB0F
UUID 564D5DF4-F404-720C-8A33-25EC4E871CB8

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



VM-Series Auth-Codes

Add VM-Series Auth-Code

VM-Series Auth-Code

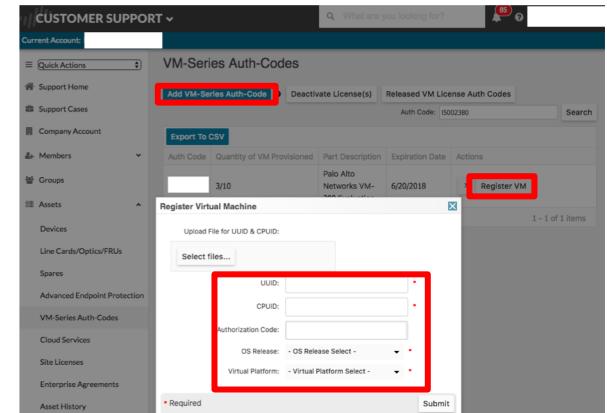
Authorization Code:

EULA

By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#).

* Required Agree and Submit Refuse

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



VM-Series Auth-Codes

Add VM-Series Auth-Code

VM-Series Auth-Codes

Palo Alto Networks VM- 6/20/2018

Register VM

Select files...

UUID:

CPUID:

Authorization Code:

OS Release: - OS Release Select -

Virtual Platform: - Virtual Platform Select -

Submit





Configure Untrust and Trust NICs

Step B3. Assign Virtual Router to Ethernet1/1

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

The left sidebar contains several categories: Interfaces (highlighted with a red box), Zones, Virtual Routers, IPsec Tunnels, DHCP, DNS, GlobalProtect (with Portals, Gateways, MDM, Device Block List, Clientless, and Clients), QoS, LLDP, and Network Profiles (with GlobalProt, IKE Gateways, IPsec Crys, IKE Crypto, Monitor, Interface, Zone Prot, QoS Prof, LLDP Prof, and BFD Prof).

The main content area has tabs for Ethernet, Loopback, and Tunnel. Under Ethernet, the interface list shows four entries: ethernet1/1, ethernet1/2, ethernet1/3, and ethernet1/4. The ethernet1/1 entry is highlighted with a red box.

A modal window titled "Ethernet Interface" is open for ethernet1/1. It displays the following fields:

- Interface Name: ethernet1/1
- Comment: (empty)
- Netflow Profile: None
- Config tab is selected.
- Assign Interface To section:
 - Virtual Router: None (highlighted with a red box)
 - Security Zone: None
 - default
- New button (highlighted with a red box)
- Virtual Router button (highlighted with a red box)
- OK and Cancel buttons at the bottom.

To the right of the interface list, a "Virtual Router" configuration window is open. It has tabs for General and ECMP. The General tab shows the following settings:

- Name: untrust-vr (highlighted with a red box)
- Administrative Distances table:

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
- Add and Delete buttons.

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

Step B4. Assign Zone to Ethernet1/1

The screenshot shows the Palo Alto Networks UI interface for assigning a security zone to an interface.

Left Panel: Shows the main navigation menu and the "Network" tab selected. Under "Network", the "Interfaces" section is active, displaying a list of Ethernet interfaces: ethernet1/1, ethernet1/2, ethernet1/3, and ethernet1/4.

Ethernet Interface Configuration: A modal window titled "Ethernet Interface" is open for "ethernet1/1".

- Interface Name:** ethernet1/1
- Comment:** (empty)
- Netflow Profile:** None
- Config Tab:** Selected
- IPv4 Tab:** Available
- Assign Interface To:** Section
 - Virtual Router:** untrust-vr
 - Security Zone:** None (highlighted with a red box)
 - Buttons:** New (disabled), Zone (highlighted with a red box)

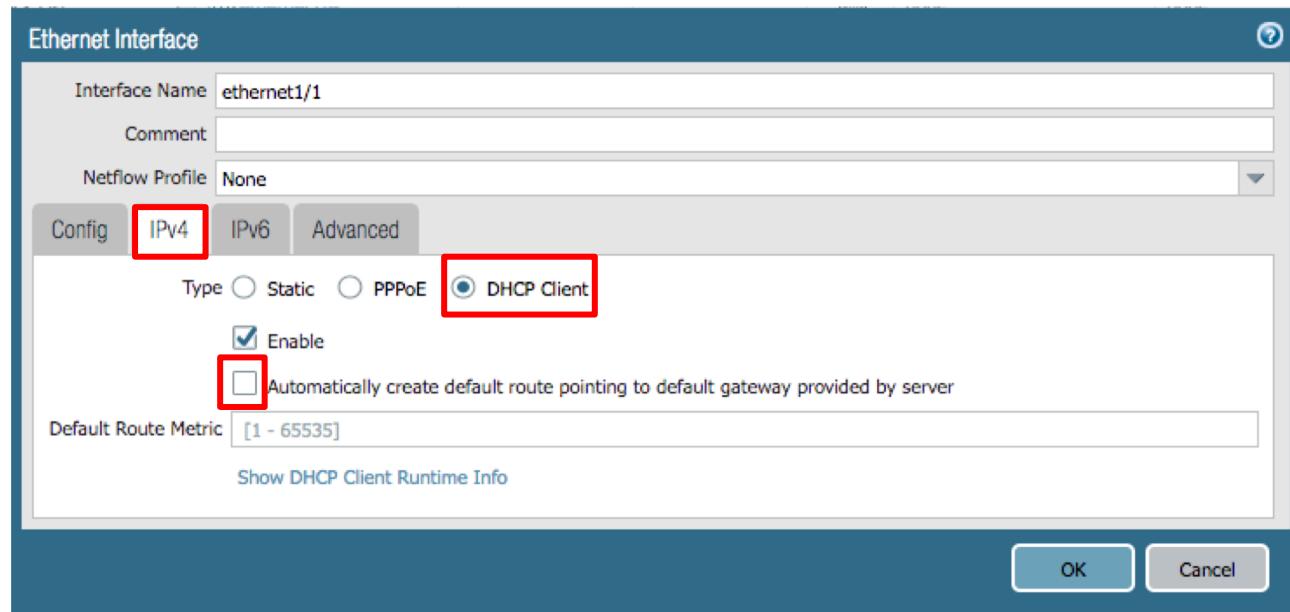
Zone Configuration: A modal window titled "Zone" is open for creating a new zone.

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

Buttons: OK, Cancel

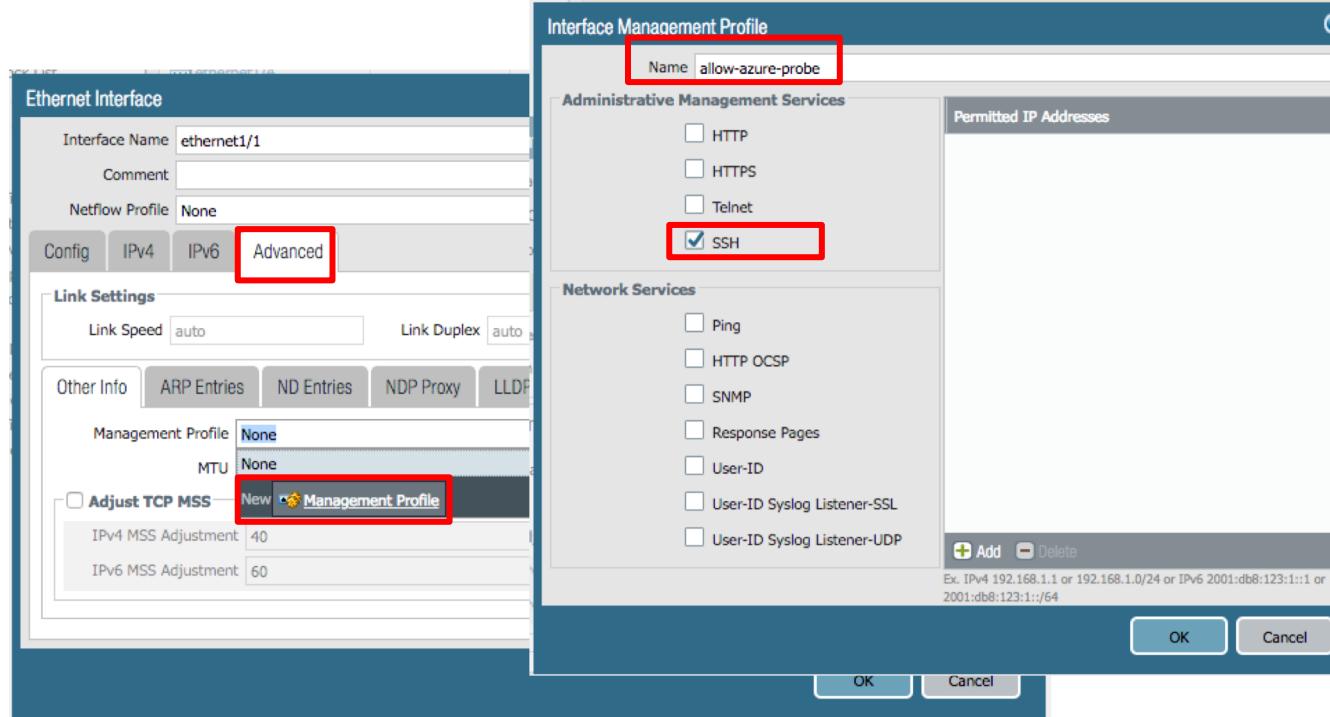
Step B5. Set Ethernet1/1 to DHCP

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



Step B6. Assign Management Profile to Ethernet1/1

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



Step B7. Assign Virtual Router to Ethernet1/2

The screenshot shows the Palo Alto Networks UI for managing network interfaces and virtual routers.

Left Sidebar: Includes links for Zones, Virtual Routers, IPsec Tunnels, DHCP, DNS, GlobalProtect, Portals, Gateways, MDM, Device Block List, Clientless, QoS, LLDP, Network Profiler, IKE Gateway, IPSec Crypto, IKE Crypto, Monitor, Interface, Zone Protection, QoS Profile, LLDP Profile, and BFD Profile.

Ethernet Interface Table: Shows a list of interfaces. The row for **Ethernet1/2** is selected and highlighted with a red box. The table columns include Interface, Interface Type, Management Profile, Link State, and several icons.

Ethernet Interface Form: A modal window for configuring Ethernet1/2. It includes fields for Interface Name (set to **Ethernet1/2**), Comment, Netflow Profile (None), and tabs for Config, IPv4, IPv6, and Advanced. Under **Assign Interface To**, the **Virtual Router** dropdown is set to **None**. The **New Virtual Router** button is highlighted with a red box.

Virtual Router Form: A modal window for creating a new virtual router named **trust-vr**. It has tabs for General and ECMP. The General tab displays the **Interfaces** section, which is currently empty. The **Administrative Distances** section lists values for various routing protocols.

Buttons: OK and Cancel buttons are located at the bottom right of the Virtual Router form.

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

Step B8. Assign Zone to Ethernet1/2

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 (highlighted)

Log Setting: None

Type: Layer3

Interfaces

Add Delete

User Identification ACL

Enable User Identification

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

Include List

Add Delete

Users from these addresses/subnets will be identified.

Exclude List

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

Zone Protection

Zone Protection Profile: None

Enable Packet Buffer Protection

OK Cancel



Step B9. Find FW-1 Management IP.

The image displays two side-by-side screenshots of the Palo Alto Networks Firewall's configuration interface, specifically for an Ethernet interface named "ethernet1/2".

Screenshot 1 (Left): Configuration Tab

- Interface Name:** ethernet1/2
- Comment:** (empty)
- Netflow Profile:** None
- Config Tab:** Selected
- Type:** Static PPPoE DHCP Client (highlighted by a red box)
- Enable:** (highlighted by a red box)
- Automatically create default route pointing to default gateway provided by:** (highlighted by a red box)
- Default Route Metric:** [1 - 65535]
- Show DHCP Client Runtime Info:** (link)

Screenshot 2 (Right): Advanced Tab

- Interface Name:** ethernet1/2
- Comment:** (empty)
- Netflow Profile:** None
- Config Tab:** Selected
- IPv4 Tab:** Selected
- Link Settings:**
 - Link Speed: auto
 - Link Duplex: auto
 - Link State: auto
- Other Info Tab:** Selected
- Management Profile:** allow-azure-probe (highlighted by a red box)
- MTU:** [undefined - 1500]
- Adjust TCP MSS:**
 - IPv4 MSS Adjustment: 40
 - IPv6 MSS Adjustment: 60
- OK** and **Cancel** buttons

Repeat these steps on FW2 using the same settings.

Configure Routing on Virtual Routers

Step C1. Go to Untrust-VR

Go to:

Network →

Virtual Routers →

untrust-vr →

Static Routes → Add

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar has tabs: Dashboard, ACC, Monitor, Policies, Objects, Network (which is highlighted with a red box), Device, Commit, and Config. The left sidebar lists various network components: Interfaces, Zones, Virtual Routers (highlighted with a red box), IPsec Tunnels, IP, DHCP, DNS, and DNS Proxy. Under GlobalParams, there are Port, Gate, MDI, Dev, Client, Client, QoS, LLDP, and Network (IKE, IPSec, IKE, BFD). The main content area shows a table of virtual routers with two entries: trust-vr (selected) and untrust-vr (highlighted with a red box). The trust-vr row shows interfaces ethernet1/2 and ethernet1/1, and ECMP status Disabled. The untrust-vr row shows interface ethernet1/1 and ECMP status Disabled. A modal window titled "Virtual Router - untrust-vr" is open. On the left of the modal is a sidebar with "Router Settings" and a list of protocols: Static Routes (highlighted with a red box), Redistribution Profile, RIP, OSPF, OSPFv3, BGP, and Multicast. The main part of the modal shows two tabs: IPv4 and IPv6. The IPv4 tab displays a table for static routes with columns: Name, Destination, Interface, Type, Value, Admin Distance, Metric, BFD, and Route Table. The table is currently empty (0 items). At the bottom of the modal, there are buttons for "+ Add" (highlighted with a red box), Delete, Clone, OK, and Cancel.

Step C2. Create 3 Routes in Untrust-VR

Virtual Router - Static Route - IPv4

Name	default-route
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

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All
Preemptive Hold Time (min)	2	

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Virtual Router - Static Route - IPv4

Name	spoke-1-route
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

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All
Preemptive Hold Time (min)	2	

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Virtual Router - Static Route - IPv4

Name	spoke-2-route
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

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All
Preemptive Hold Time (min)	2	

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Untrust-VR Route Summary

Virtual Router - untrust-vr

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

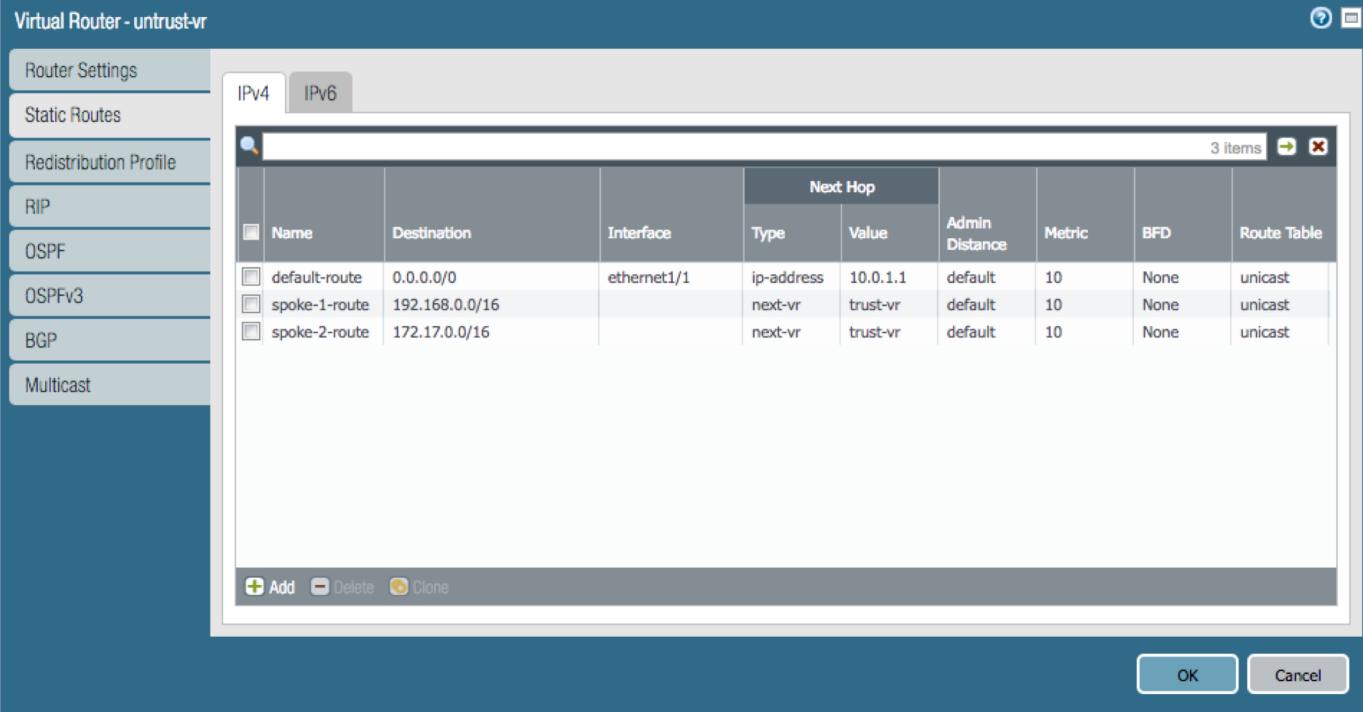
IPv4 IPv6

3 items

Name	Destination	Interface	Next Hop		Admin Distance	Metric	BFD	Route Table
			Type	Value				
default-route	0.0.0.0/0	ethernet1/1	ip-address	10.0.1.1	default	10	None	unicast
spoke-1-route	192.168.0.0/16		next-vr	trust-vr	default	10	None	unicast
spoke-2-route	172.17.0.0/16		next-vr	trust-vr	default	10	None	unicast

Add Delete Clone

OK Cancel



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

Step C3. Go to Trust-VR

Go to:

Network →

Virtual Routers →
trust-vr →

Static Routes → Add

The screenshot shows the Palo Alto Networks Firewall UI with the following interface details:

- Top Navigation Bar:** Dashboard, ACC, Monitor, Policies, Objects, **Network** (highlighted with a red box), Device, Commit, Config, Search.
- Left Sidebar:** AAA, Interfaces, Zones, **Virtual Routers** (highlighted with a red box), IPSec Tunnels, IP DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Device Block, Clientless Apps, Clientless Apps, QoS, LLDP, Network Profiles, GlobalProtect, IKE Gateway, IKE Crypto, Monitor, Interface Mgt, Zone Protect, QoS Profile, LLDP Profile, BFD Profile.
- Virtual Router List:** default (disabled), untrust-vr (selected, highlighted with a red box), trust-vr (selected, highlighted with a red box).
- Virtual Router - trust-vr Dialog:**
 - Router Settings:** Static Routes (highlighted with a red box).
 - Static Routes:** IP4 tab, IPv6 tab, 0 items.
 - Add Route:** Add, Delete, Clone.
 - Buttons:** OK, Cancel.
- Palo Alto Networks Logo:** In the bottom right corner.

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

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

Path Monitoring

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Add Delete

OK Cancel

Virtual Router - Static Route - IPv4

Name	spoke-1-route
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

Path Monitoring

Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Add Delete

OK Cancel

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

Virtual Router - Static Route - IPv4

Name	spoke-2-route
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

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All	Preemptive Hold Time (min)	2	
Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Add Delete

OK Cancel

Virtual Router - Static Route - IPv4

Name	azure-lb-route
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

Path Monitoring

Failure Condition	<input checked="" type="radio"/> Any	<input type="radio"/> All	Preemptive Hold Time (min)	2	
Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

Add Delete

OK Cancel

Trust-VR Route Summary

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

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-route	192.168.0.0/16	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
spoke-2-route	172.17.0.0/16	ethernet1/2	ip-address	10.0.2.1	default	10	None	unicast
azure-lb-route	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 exact routes.



Configure NAT Policies

NAT Policy Overview

We need to create 4 NAT Policies.

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

The screenshot shows the Palo Alto Networks interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (which is highlighted with a red box), Objects, Network, and Device. On the left, a sidebar under the Security section has icons for NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The NAT icon is also highlighted with a red box. The main content area displays a table with columns for Name, Tags, Source Zone, Destination Zone, and Destination Interface. At the bottom of the table is an 'Add' button with a plus sign, also highlighted with a red box. The footer contains links for paloalto | Logout | Last Login Time: 11/12/2018 15:22:13 and buttons for PDF/CSV, Highlight Unused Rules, and Refresh.

Step D1. Create No-NAT Policy for Azure Probe

NAT Policy Rule

General Original Packet Translated Packet

Name: no-nat-on-azure-probe

Description:

Tags:

NAT Type: ipv4

NAT Policy Rule

General Original Packet Translated Packet

Source Zone: Any

Destination Zone: untrust-zone

Source Address: Any

Destination Address: Any

168.63.129.16/32

Destination Interface: any

Service: any

Source Address Translation

Translation Type: None

Destination Address Translation

Translation Type: None

OK Cancel

Step D2. Create DNAT Policy to Web-LB

NAT Policy Rule

General Original Packet Translated Packet

Name: inbound-to-web-server

Description:

Tags:

NAT Type: ipv4

NAT Policy Rule

General Original Packet Translated Packet

Source Zone: untrust-zone

Destination Zone: untrust-zone

Source Address:

Destination Address: 10.0.1.4

Destination Interface: any

Service: service-http

Add Delete

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: Dynamic IP (with session distribution)

Translated Address: 192.168.0.100

Translated Port: 80

OK Cancel

Step D3. Create DNAT Policy to Jump VM

The screenshot shows the configuration of a NAT Policy Rule across three tabs: General, Original Packet, and Translated Packet.

General Tab:

- Name: inbound-to-jump-server (highlighted by a red box)
- Description: (empty)
- Tags: (empty)
- NAT Type: ipv4

Original Packet Tab:

- Source Zone: untrust-zone (highlighted by a red box)
- Destination Zone: Any
- Source Address: Any
- Destination Address: 10.0.1.4 (highlighted by a red box)
- Destination Interface: any
- Service: any

Translated Packet Tab:

- Source Address Translation:
 - Translation Type: Dynamic IP And Port (highlighted by a red box)
 - Address Type: Interface Address
 - Interface: ethernet1/2
 - IP Address: None
- Destination Address Translation:
 - Translation Type: Static IP (highlighted by a red box)
 - Translated Address: 172.17.0.4
 - Translated Port: 22

OK and Cancel buttons are visible at the bottom right of the main window.

Step D4. Create SNAT Policy for Internet

NAT Policy Rule

General Original Packet Translated Packet

Name: outbound-internet

Description:

Tags:

NAT Type: ipv4

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

NAT Policy Rule

General Original Packet Translated Packet

Source Address Translation

Translation Type: Dynamic IP And Port

Address Type: Interface Address

Interface: ethernet1/1

IP Address: None

Destination Address Translation

Translation Type: None

OK Cancel

The screenshot illustrates the configuration of a NAT Policy Rule for Internet access. The rule is named "outbound-internet" and is set to use the "trust-zone" as the source zone and the "untrust-zone" as the destination zone. The "Original Packet" tab is active. In the "Source Address Translation" section, the "Translation Type" is set to "Dynamic IP And Port", "Address Type" is "Interface Address", and the "Interface" is "ethernet1/1". The "IP Address" field is set to "None". The "Translated Packet" tab is also present.

NAT Policy Summary

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

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

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



Configure Security Policies
&
Commit Changes

Step E1. Create a New Security Policy

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

THIS IS TEMPORARY FOR TESTING PURPOSES ONLY.

The screenshot shows the Palo Alto Networks management interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (which is highlighted with a red box), Objects, Network, and Device. On the left, a sidebar under the 'Security' heading lists NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main content area displays a table of existing security policies:

	Name	Tags	Type	Zone	Address	U
1	intrazone-default	none	intrazone	any	any	a
2	interzone-default	none	interzone	any	any	a

At the bottom of the table, there are buttons for Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, and Help. The status bar at the bottom indicates the user is 'paloalto' and last logged in on 11/12/2018 at 15:22:13.

Step E2. Configure the Security Policy

The screenshot shows three overlapping windows for configuring a security policy rule.

Top Window (Main Configuration):

- General Tab:** Name: test-allow-all (highlighted with a red box), Rule Type: universal (default), Description: Temporary rule to allow all traffic for testing.
- Source Tab:** Destination is selected (highlighted with a red box). Under Destination, the "Any" checkbox is checked (highlighted with a red box).
- Destination Tab:** Source Zone is selected. Under Source Zone, the "any" dropdown is set to "any" (highlighted with a red box).

Bottom Window (Details):

- General Tab:** Destination is selected. Under Destination, the "Any" checkbox is checked.
- Destination Tab:** Destination Zone is selected. Under Destination Zone, the "any" dropdown is set to "any".

Buttons at the Bottom:

- OK** button (highlighted with a red box) and **Cancel** button.

Security Policy Summary

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

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

Step E3. Commit all our Changes

The screenshot shows the Palo Alto Networks Firewall interface. The top navigation bar includes links for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, Device, and a redboxed Commit button. A sidebar on the left lists security-related options like NAT, QoS, Policy Based Forwarding, and Tunnel Inspection. The main pane displays a table of policy rules:

Name	Tags	Type	Zone	Address	User	HIP Profile	Zon
1 test-allow-all	none	universal	any	any	any	any	any
2 intrazone-default	none	intrazone	any	any	any	any	(int

A modal dialog titled "Commit" is open, containing the following text: "Doing a commit will overwrite the running configuration with the commit scope." It features two radio buttons: "Commit All Changes" (selected) and "Commit Changes Made By:(1) paloalto". Below this is a "Commit Scope" section with two entries: "policy-and-objects" and "device-and-network". At the bottom of the dialog are buttons for "Preview Changes", "Change Summary", "Validate Commit", "Group By Location Type", "Commit" (which is also redboxed), and "Cancel".

Tag Browser panel on the left shows 1 item with a table:

Tag(#)	Rule
none (1)	1

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

Repeat these steps for FW2.



Test the Deployment

Step F1. Find Public LB Public IP

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

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu is visible with the 'All resources' option selected. In the center, the 'All resources' blade shows a list of resources, with 'firewall-public-lb' highlighted. To the right, the detailed view for 'firewall-public-lb' is displayed, specifically the 'Overview' tab. Key information shown includes:

- Resource group: palo-test-rg
- Location: East US
- Subscription name: Visual Studio Professional
- Subscription ID: 36a6952c-125c-4b32-943e-27e85b91d591
- SKU: Standard
- Backend pool: firewall-untrust-pool (2 virtual machines)
- Health probe: tcp-22 (TCP:22)
- Load balancing rule: frontend-ip-1 (TCP/80)
- NAT rules: -
- Public IP address: 104.45.173.74 (public-lb-pip)

Step F2. SSH into VM and test Traffic Flows.

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

Hostname: Your-Public-LB-IP

Username: paloalto

Password: PanPassword123!

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

Step 2. Try pinging out to the internet

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

Step 3. Try pinging to the other Spoke VNET

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



Step F3. SSH into Web VM and install Apache

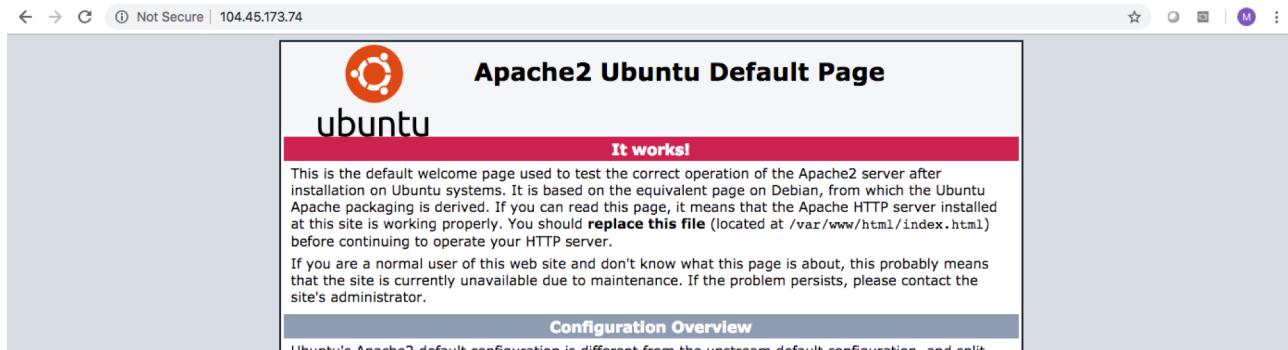
Step 1. While in the jump-vm, SSH to the Web-VM in Spoke-1-VNET

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

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

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

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



Step F4. Filter Firewall Traffic Logs for your tested Traffic

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

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. Below the navigation bar is a search bar containing the filter '(addr in 192.168.0.4)'. On the left, a sidebar under the 'Logs' section has 'Traffic' selected (also highlighted with a red box). 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. The table contains five log entries:

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

If you do not see logs, check FW2.

Thank you!

