

# Palo Alto Networks

## Azure Active/Passive Guide

Matt McLimans, Public Cloud Consultant Engineer

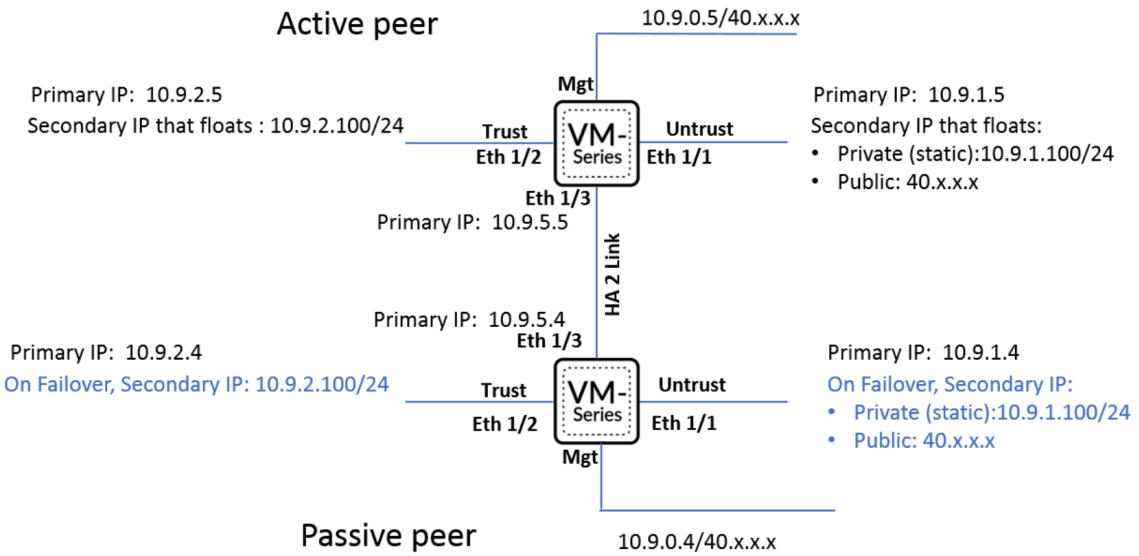


# SUPPORT POLICY

This is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself. Unless explicitly tagged, all projects or work posted in our GitHub repository (at <https://github.com/PaloAltoNetworks>) or sites other than our official Downloads page on <https://support.paloaltonetworks.com> are provided under the best effort policy.

# DEPLOYMENT OVERVIEW

- This is a deployment guide 2xVM-Series firewalls in an Active/Passive pair.
- This deployment aims to replicate the architecture in:  
[Set up Active/Passive HA on Azure.](#)



# STEP 1. LAUNCH TEMPLATE

1. Launch the ARM Template

[https://github.com/wwce/azure-arm/tree/master/Azure-CommonDeployments/v1/2fw\\_3nic\\_avset\\_active\\_passive](https://github.com/wwce/azure-arm/tree/master/Azure-CommonDeployments/v1/2fw_3nic_avset_active_passive)

2. Download **active-fw-config.xml** & **passive-fw-config.xml**. The firewall configurations are configured to reflect the default parameter settings.



## STEP 2. USER REQUIRED PARAMETERS

**Resource Group:** Create a new Resource Group

*All resources deployed in template will belong to Resource Group selected.*

**License Type:** Select BYOL / Bundle1 / Bundle2

**Username:** Enter username (do not use admin or root)

**Password:** Enter password.

**BASICS**

* Subscription	Pay-As-You-Go
* Resource group	(New) vmseries-rg <a href="#">Create new</a>
* Location	(US) East US

* License Type ⓘ	bundle2
PANOS Version ⓘ	latest

Username ⓘ	paloalto
* Password ⓘ	*****



# STEP 3. VERIFY DEPLOYMENT & OPEN RESOURCE GROUP

- Once the deployment completes, open the Resource Group.

The screenshot shows two side-by-side views of the Azure portal. On the left is the Notifications blade, which displays a deployment event: "Deployment in progress..." for resource group 'vmseries-rg' started 2 minutes ago. A red box highlights the bell icon in the top bar of the Notifications blade. An orange arrow points from the "Deployment in progress..." message in the Notifications blade to the "Your deployment is complete" message on the Microsoft.Template - Overview page. On the right is the Microsoft.Template - Overview page, showing deployment details and a table of operation results.

**Notifications**

More events in the activity log →

Dismiss all ...

Deployment in progress...

Running

Deployment to resource group 'vmseries-rg' is in progress.

2 minutes ago

**Microsoft.Template - Overview**

Home > Microsoft.Template - Overview

Microsoft.Template - Overview

Deployment

Search (Ctrl+ /)

Delete Cancel Redeploy Refresh

Overview Inputs Outputs Template

Your deployment is complete

Check the status of your deployment, manage resources, or troubleshoot deployment issues. Pin this page.

Deployment name: Microsoft.Template  
Subscription: Pay-As-You-Go  
Resource group: vmseries-rg

DEPLOYMENT DETAILS (Download)

Start time: 5/25/2019, 11:46:26 AM  
Duration: 7 minutes 32 seconds  
Correlation ID: 059a9526-1a06-4da4-9de7-987ad397174a

RESOURCE	TYPE	STATUS	OPERATION DETAILS
CREATE_FW2	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_FW1	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_VM	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_VNET	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_ROUTE_TABLE	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_AVSET	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>
CREATE_NSGS	Microsoft.Resources/deployments	OK	<a href="#">Operation details</a>

# CONFIGURE **ACTIVE FIREWALL**

# STEP 4. ACCESS ACTIVE FW GUI

1. Resource Group → Overview → **vmseries-active-nic0-pip**

The screenshot shows the Azure Resource Group Overview page for 'vmseries-rg'. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Events, Quickstart, Deployments, Policies, Properties, and Locks. The main area displays resource details: Subscription (Pay-As-You-Go), Subscription ID (8c3495af-c1a6-4e0a-b32d-af967144b456), and Tags. Below this is a list of resources, with 'vmseries-active-nic0-pip' highlighted by a red box. The list includes:

NAME	TYPE
vmseries-active-nic1	Network interface
<b>vmseries-active-nic0-pip</b>	Public IP address
vmseries-active-nic0	Network interface

2. Copy public IP Address

The screenshot shows the Azure Resource Group Overview page for 'vmseries-rg'. The 'Overview' tab is selected. On the right, detailed information is shown for the Public IP address 'vmseries-active-nic0-pip':

Resource group (change)	SKU
vmseries-rg	Basic
Location	East US
Subscription (change)	Pay-As-You-Go
IP address	52.191.215.9
DNS name	-

3. Paste into URL [https://<public\\_ip>](https://<public_ip>)  
Login with username & password from Step 2

The screenshot shows a web browser window with the URL 'https://52.191.215.9' in the address bar. The page itself is a Palo Alto Networks login screen, featuring the Palo Alto Networks logo and fields for 'Username' (paloalto) and 'Password'. A blue 'Log In' button is at the bottom.



# STEP 5. IMPORT & LOAD CONFIGURATION

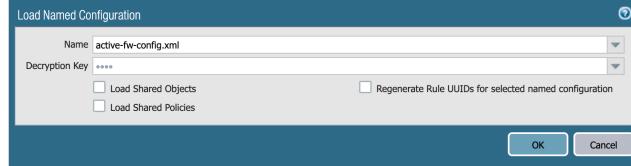
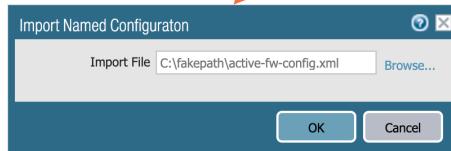
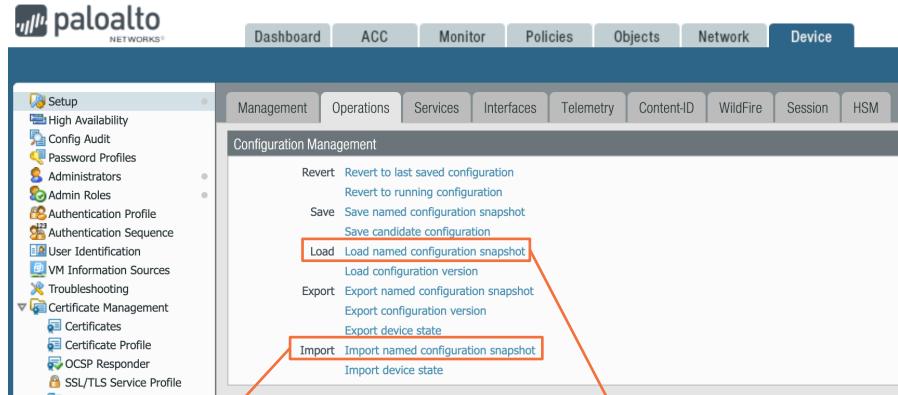
Device → Setup → Operations

→ Import named configuration snapshot

→ select **active-fw-config.xml**

→ Load named configuration snapshot

→ select **active-fw-config.xml**



# STEP 6. ENABLE HA

Device → High Availability

→ General → Setup

→ Check on **Enable HA**

The screenshot shows the Palo Alto Networks Device Management interface. The left sidebar menu is expanded, showing various configuration categories like Setup, High Availability, Config Audit, and others. The 'High Availability' option is selected and highlighted with a red box. The main content area has two tabs at the top: 'General' and 'Operational Commands', with 'General' selected. On the left under 'General', there is a 'Setup' section containing several configuration fields. One of these fields, 'Enable HA' (checkbox), is also highlighted with a red box. Other fields in this section include 'Group ID 1', 'Mode active-passive', 'Enable Config Sync' (checkbox), and 'Peer HA1 IP Address 10.9.0.4'. To the right of the 'Setup' section are two panels: 'Control Link (HA1)' and 'Data Link (HA2)'. The 'Control Link (HA1)' panel shows port management settings like 'Port management', 'Encryption Enabled' (unchecked), and 'Monitor Hold Time (ms) 3000'. The 'Data Link (HA2)' panel shows session synchronization settings like 'Enable Session Synchronization' (checkbox checked), 'Port ethernet1/3', and 'IPv4/IPv6 Address 10.9.5.5'. At the bottom of the page, the URL is https://52.191.215.9/#, and the footer includes links for initial, Tasks, and Language.

# CREATE AZURE SERVICE PRINCIPAL (skip if you already have one)

Please see:

- [Application and service principal objects in Azure Active Directory](#)
- [Create an Azure service principal with Azure CLI](#)

## 1. Log into Azure CLI

```
> az login
```

## 2. Create service principal

```
> az ad sp create-for-rbac --name vmseries-HA
{
    "appId": "17c*****-****-****-****-*****061",      ← Client ID
    "displayName": "vmseries-HA",
    "name": "http://vmseries-HA",
    "password": "*a36*****-****-****-****-*****97b",   ← Client Secret
    "tenant": "52f*****-****-****-****-*****b28"       ← Tenant ID
}
```

## 3. Verify role

```
> az role assignment list --assignee 17c*****-****-****-****-*****061
[
    {
        "canDelegate": null,
        "id": "/subscriptions/<subscription_id>/providers/Microsoft.Authorization/roleAssignments/<redacted>",
        "name": "<redacted>",
        "principalId": "<redacted>",
        "principalName": "http://vmseries-HA",
        "roleDefinitionId": "<redacted>",
        "roleDefinitionName": "Contributor",   ← Valid role
        "scope": "<redacted>",
        "type": "Microsoft.Authorization/roleAssignments"
    }
]
```



# STEP 7. CONFIGURE AZURE HA PLUGIN

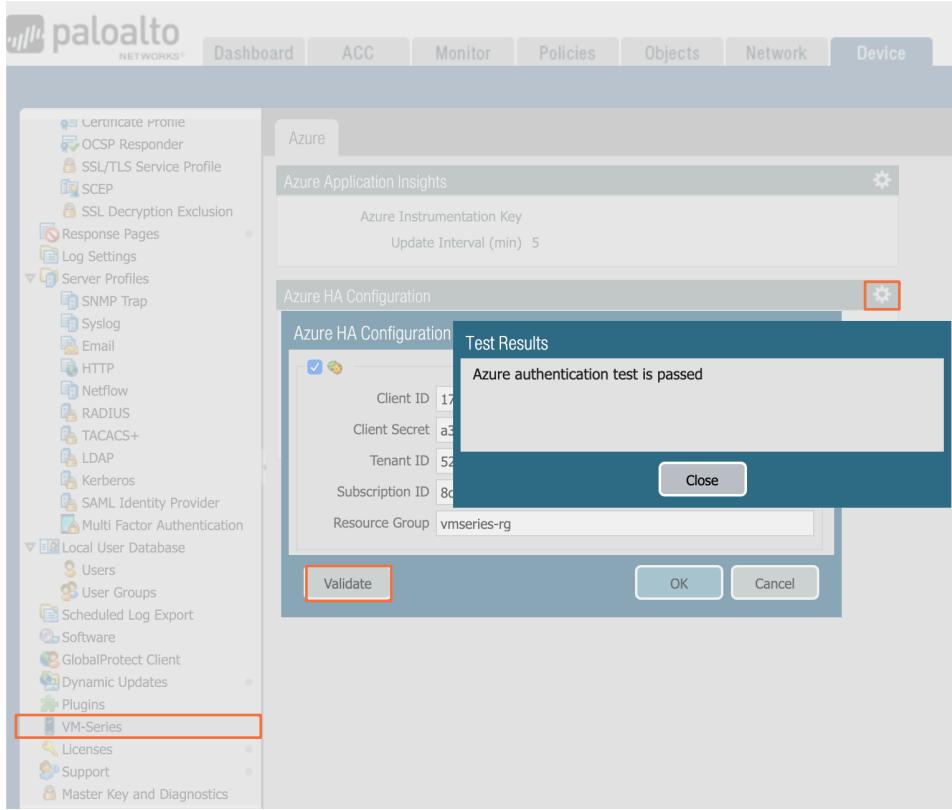
1. Device → VM-Series → Azure HA Configuration  
→ Enter your Azure service principal parameters

2. Click **Validate** to test plugin authentication.

**COMMIT CHANGES**

The imported configuration has a default username & password

**UN:paloalto / PW:PanPassword123!**



# CONFIGURE **PASSIVE** FIREWALL

# STEP 8. ACCESS PASSIVE FW GUI

## 1. Overview → **vmseries-passive-nic0-pip**

The screenshot shows the Azure Resource Groups overview page for the 'vmseries-rg' resource group. The 'Overview' tab is selected. Key details shown include:

- Subscription (change): Pay-As-You-Go
- Subscription ID: 8c3495af-c1a6-4e0a-b32d-af967144b456
- Tags (change): Click here to add tags
- Deployments: 8 Succeeded
- Network interface: vmseries-passive-nic0 (Type: Network interface, Location: East US)
- Public IP address: vmseries-passive-nic0-pip (Type: Public IP address, Location: East US)
- Network interface: vmseries-passive-nic0 (Type: Network interface, Location: East US)

## 2. Copy public IP Address

The screenshot shows the Azure Resource Group details page for 'vmseries-passive-nic0-pip'. The 'Overview' tab is selected. Key details shown include:

- Resource group (change): vmseries-rg
- SKU: Basic
- Location: East US
- Subscription (change): Pay-As-You-Go
- DNS name: -
- IP address: 40.114.65.84

## 3. Paste into URL [https://<public\\_ip>](https://<public_ip>) Login with username & password from Step 2

The screenshot shows a web browser displaying the Palo Alto Networks login page. The URL is https://40.114.65.84/php/login.php. The page features the Palo Alto Networks logo and fields for Username (paloalto) and Password, with a Log In button.



# STEP 9. IMPORT & LOAD CONFIGURATION

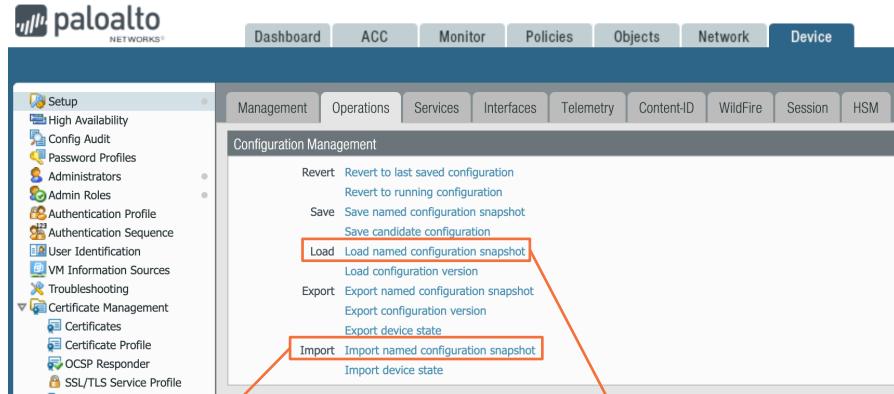
Device → Setup → Operations

→ Import named configuration snapshot

→ select **passive-fw-config.xml**

→ Load named configuration snapshot

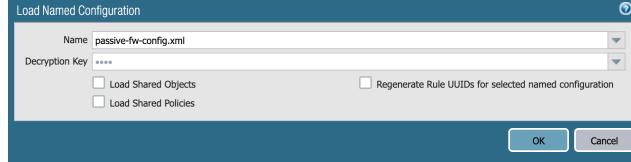
→ select **passive-fw-config.xml**



## COMMIT CHANGES

The imported configuration has a default username & password

UN:paloalto / PW:PanPassword123!



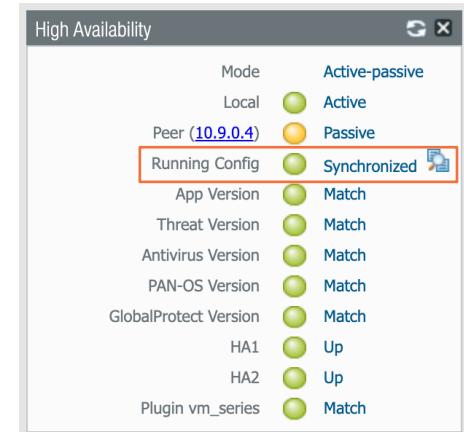
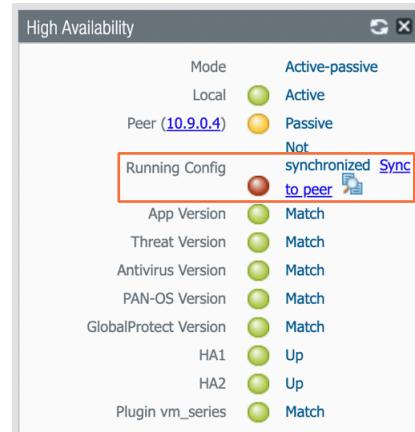
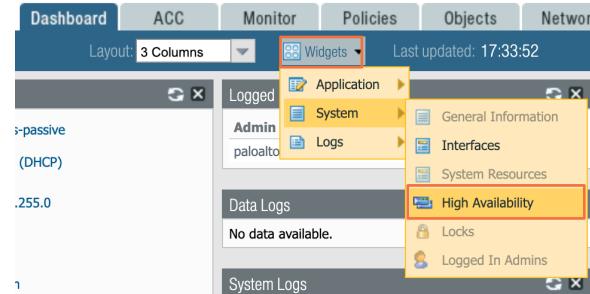
# STEP 10. SYNC ACTIVE FW WITH PASSIVE FW

1. On both firewalls, enable the High Availability Widget

Dashboard → Widgets

→ System → High Availability

2. On the **Active firewall**, click **Sync to peer**.



# TEST FAILOVER

# VERIFY UNTRUST FLOATING IP ON ACTIVE FW

1. In the Azure portal, open the IP configurations for **vmseries-active-nic1** and **vmseries-passive-nic1**
2. The floating IP (10.9.1.100) resides on **vmseries-active-nic1**.

Home > vmseries-rg > vmseries-active-nic1 - IP configurations

### vmseries-active-nic1 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings

IP forwarding  Enabled

Virtual network **vmseries-vnet**

IP configurations

\* Subnet **untrust-subnet (10.9.1.0/24)**

Search IP configurations				
NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.1.5 (Static)	-
<b>floating</b>	IPv4	Secondary	10.9.1.100 (Static)	40.114.65.11 (ymseries-activ... ...)

**ACTIVE**  
(before failover)

Home > vmseries-rg > vmseries-passive-nic1 - IP configurations

### vmseries-passive-nic1 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings

IP forwarding  Disabled  Enabled

Virtual network **vmseries-vnet**

IP configurations

\* Subnet **untrust-subnet (10.9.1.0/24)**

Search IP configurations				
NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.1.4 (Static)	-
				...

**PASSIVE**  
(before failover)

# VERIFY TRUST FLOATING IP ON ACTIVE FW

1. In the Azure portal, open the IP configurations for **vmseries-active-nic2** and **vmseries-passive-nic2**
2. The floating IP (10.9.2.100) resides on **vmseries-active-nic2**.

Home > vmseries-rg > vmseries-active-nic2 - IP configurations

### vmseries-active-nic2 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings

IP forwarding: Enabled

Virtual network: vmseries-vnet

IP configurations

\* Subnet: trust-subnet (10.9.2.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.2.5 (Static)	-
<b>floating</b>	IPv4	Secondary	10.9.2.100 (Static)	-

**ACTIVE**  
(before failover)

Home > vmseries-rg > vmseries-passive-nic2 - IP configurations

### vmseries-passive-nic2 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings

IP forwarding: Enabled

Virtual network: vmseries-vnet

IP configurations

\* Subnet: trust-subnet (10.9.2.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.2.4 (Static)	-

**PASSIVE**  
(before failover)

# INITIATE A FAILOVER

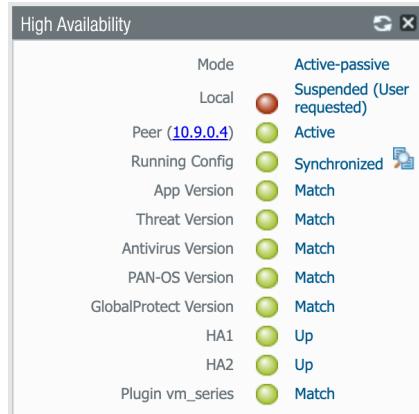
1. On the **Active firewall**, go to:

Device → High Availability → Operational Commands

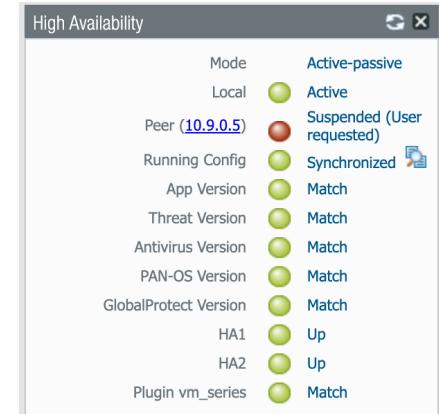
→ click **Suspend local device**



2. View the High Availability widget. The passive firewall should now be Active.



**ACTIVE**  
(after failover)



**PASSIVE**  
(after failover)

# VERIFY UNTRUST FLOATING IP MOVE TO PASSIVE FW

1. In the Azure portal, open the IP configurations for **vmseries-active-nic1** and **vmseries-passive-nic1**
2. The floating IP (10.9.1.100) should now belong to **vmseries-passive-nic1**

Home > vmseries-rg > vmseries-active-nic1 - IP configurations

### vmseries-active-nic1 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings  
IP forwarding  Disabled  Enabled

Virtual network **vmseries-vnet**

IP configurations  
\* Subnet **untrust-subnet (10.9.1.0/24)**

Search IP configurations

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.1.5 (Static)	-
				...

**ACTIVE**  
**(after failover)**

Home > vmseries-rg > vmseries-passive-nic1 - IP configurations

### vmseries-passive-nic1 - IP configurations

Network interface

+ Add Save Discard

IP forwarding settings  
IP forwarding  Disabled  Enabled

Virtual network **vmseries-vnet**

IP configurations  
\* Subnet **untrust-subnet (10.9.1.0/24)**

Search IP configurations

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.1.4 (Static)	-
				...
<b>floating</b>	<b>IPv4</b>	<b>Secondary</b>	<b>10.9.1.100 (Static)</b>	<b>40.114.65.11 (vmseries-activ... ...)</b>

**PASSIVE**  
**(after failover)**

# VERIFY TRUST FLOATING IP MOVE TO PASSIVE FW

1. In the Azure portal, open the IP configurations for **vmseries-active-nic2** and **vmseries-passive-nic2**
2. The floating IP (10.9.2.100) should now belong to **vmseries-passive-nic2**

Home > vmseries-rg > vmseries-active-nic2 - IP configurations

### vmseries-active-nic2 - IP configurations

Network interface

**IP forwarding settings**  
IP forwarding

**Virtual network** vmseries-vnet

**IP configurations**

\* Subnet trust-subnet (10.9.2.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.2.5 (Static)	-

ACTIVE  
(after failover)

Home > vmseries-rg > vmseries-passive-nic2 - IP configurations

### vmseries-passive-nic2 - IP configurations

Network interface

**IP forwarding settings**  
IP forwarding

**Virtual network** vmseries-vnet

**IP configurations**

\* Subnet trust-subnet (10.9.2.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
primary	IPv4	Primary	10.9.2.4 (Static)	-
floating	IPv4	Secondary	10.9.2.100 (Static)	-

PASSIVE  
(after failover)