



Azure Two-Tier ARM Template Deployment Guide

<http://www.paloaltonetworks.com>

Table of Contents

- 1. About ARM Templates 3**
- 2. Prerequisites 4**
 - 2.1 Create an Azure account 4
 - 2.2 Add a credit card to your Azure account 5
- 3. Launch The ARM Template 6**
 - 3.1 Deploy from github 6
 - 3.2 The Parameters 8
 - 3.3 Review and Launch 11
 - 3.4 Check Deployment Status 12
 - 3.5 Deployment failed 14
 - 3.6 Deployment successful 15
- 4. Overview of Resources Created 16**
- 5. Configure the VM-Series and Secure Traffic 20**
- 6. Cleanup 22**

1. About ARM Templates

Azure Resource Manager (ARM) templates are JSON files that can launch nearly all Azure resources including VNets, subnets, security groups, route tables and more.

For more information regarding ARM templates please refer to the Azure documentation here:

<https://azure.microsoft.com/en-us/documentation/articles/resource-group-overview/>

There are also many sample templates available here:

<https://azure.microsoft.com/en-us/documentation/templates/>

Azure currently supports the ability to deploy a virtual machine with only one network interface using the Azure UI. Launching a virtual machine with multiple interfaces requires templates. To simplify the process of deploying the VM-Series firewall with multiple interfaces, Palo Alto Networks provides an ARM template.

This document will explain how to deploy a sample template for a simple, two-tiered application framework including a VM-Series firewall. The template will launch everything that is shown in Figure 1 below. The ARM template includes the following components to help deploy the firewall as a gateway for Internet-facing applications— a VM-Series firewall, a small Linux virtual machine that performs NAT and two Linux virtual machines that you can configure as a two-tiered application such as a web server and a database server. The template also includes the functions to create the VNet and subnets within the resource group, and adds the necessary user-defined routes (UDRs) and IP forwarding flags to enable the VM-Series firewall to secure the Azure resource group.

Sample templates provided by Palo Alto Networks including the one this document references can be found here:

<https://github.com/PaloAltoNetworks/azure/>

The template deploys the following virtual machines within a VNET:

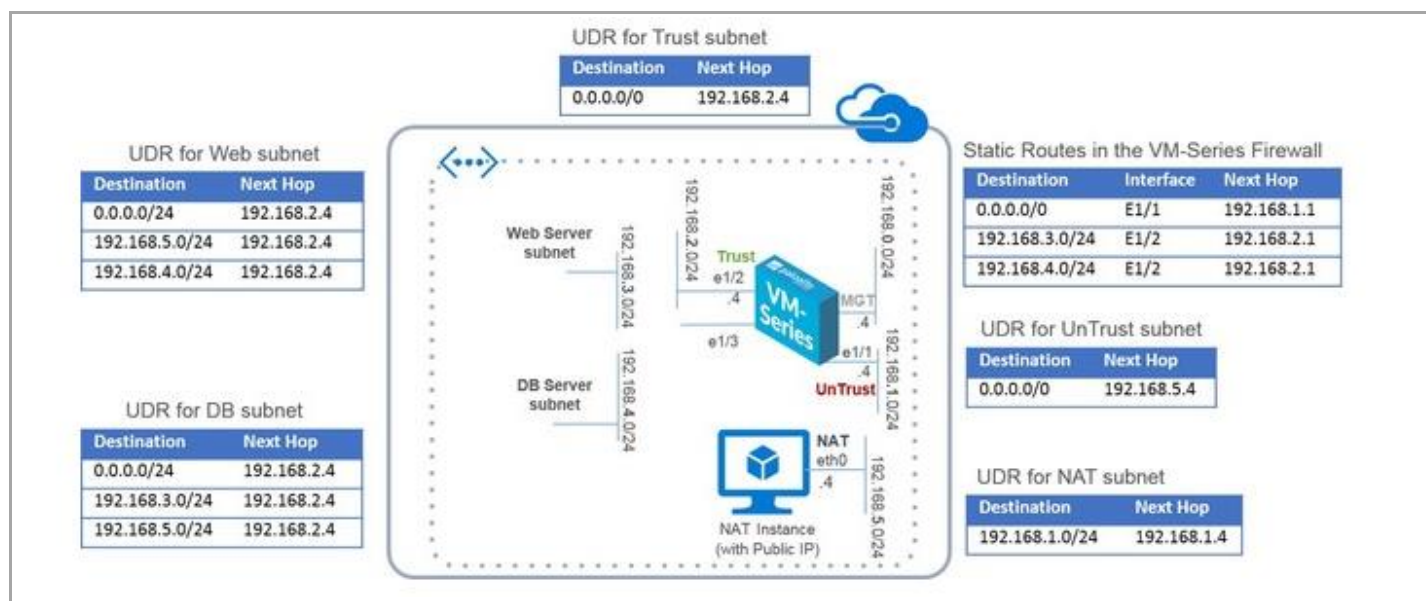


Figure 1: Template topology

For detailed documentation regarding the template and configuration of the VM Series firewall, please refer to the following document:

<https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/set-up-the-vm-series-firewall-in-azure>

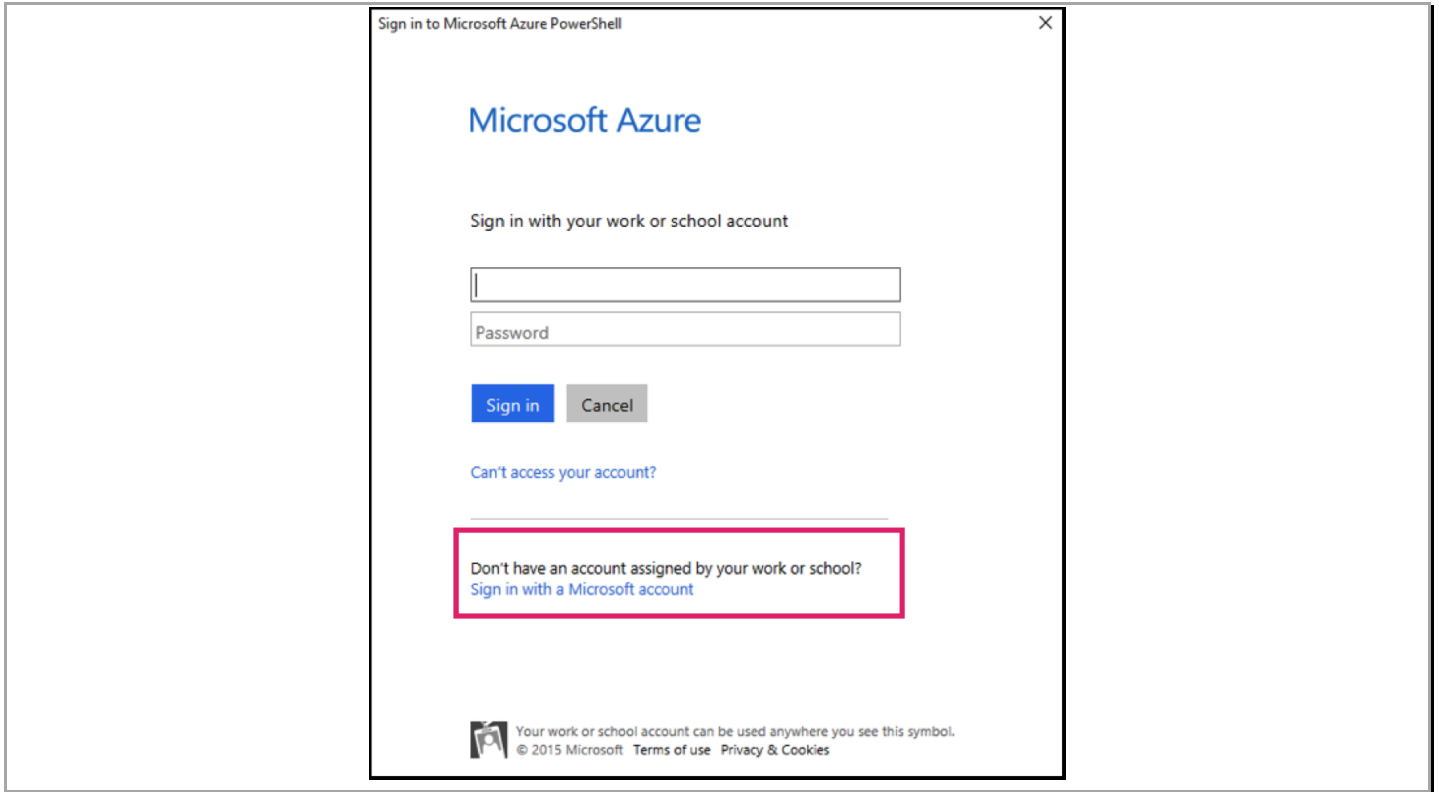
2. Prerequisites

Here are the prerequisites required to successfully launch this template.

2.1 Create an Azure account

If you do not have an Azure account already, go to <https://azure.microsoft.com/en-us/pricing/free-trial/> and create an account. If you already have an Azure account please proceed to [Section 3](#)

Create the account as a "Microsoft account" (also known as a Live ID or Hotmail account) and not a "for work or school account".



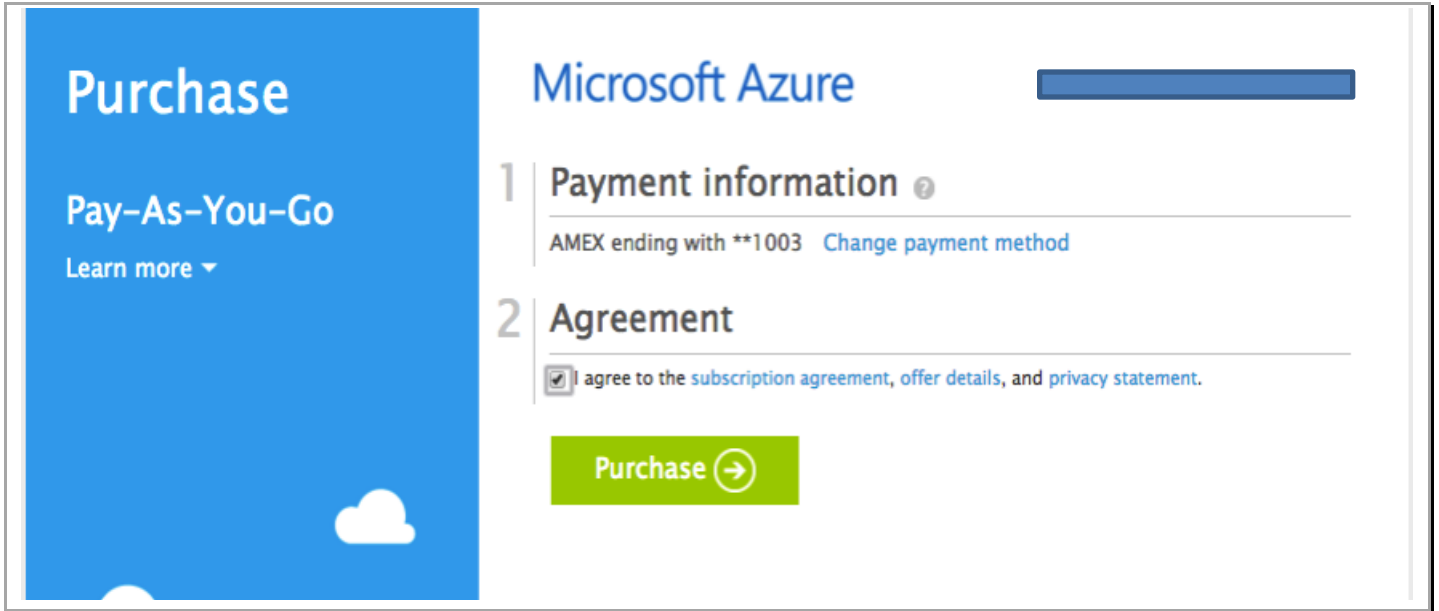
The free trial expires 30 days from account creation date or when \$200 free credits are used up.

2.2 Add a credit card to your Azure account

In order to launch the VM Series firewall (or anything with more than 4 cores) you will need to add a method of payment to your Azure account. For details, see: <https://msdn.microsoft.com/en-us/library/azure/dn736057.aspx>

Once done, request Microsoft to switch to the subscription to use the Pay-As-You-Go subscription (as opposed to the free one). This usually takes 3 to 4 days to complete.

Optionally, you can directly add a new subscription. To do so go to <https://account.windowsazure.com/Subscriptions> and click **“add subscription”** and select **“Pay-As-You-Go”**, Add payment details, check the box to agree to the terms and conditions and click **“Purchase”**



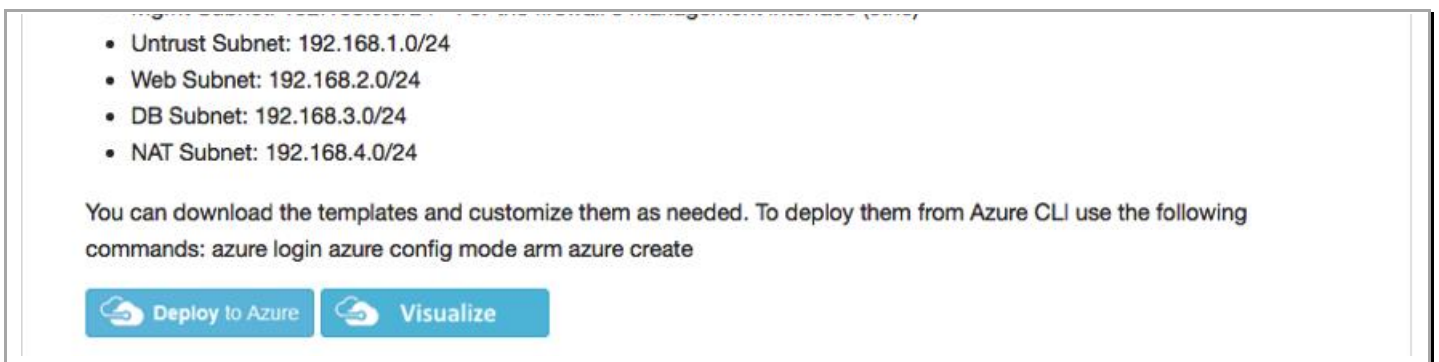
3. Launch The ARM Template

3.1 Deploy from github

This document covers how to launch the template from the Azure portal. For details on using the Azure command line please refer to following doc

<https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/set-up-the-vm-series-firewall-in-azure/use-the-arm-template-to-deploy-the-vm-series-firewall>

Navigate to <https://github.com/PaloAltoNetworks/azure/tree/master/vmseries-nat-webdb> to access the ARM template.



Click “**Visualize**” for a visual representation of the various resources the template launches.

Palo Alto Networks Azure ARM Template Deployment Guide

Click **“Deploy to Azure”** link. You will be prompted to log in to your Azure account and prompted to specify some template parameters.

Microsoft Azure

New > New > Custom deployment > Parameters

Custom deployment
Deploy from a custom template

Parameters
Customize your template parameters

Template
Edit template

Parameters
Edit parameters

Subscription
Narayan-pay-as-you-go

Resource group
+ New

New resource group name

Resource group location
East US

Legal terms
Review legal terms

☐ Pin to dashboard

Create

USERIMAGESTORAGEACCOUNTNAME (string)

DNSNAMEFORPUBLICIP (string)

DNSNAMEFORPUBLICIPNAT (string)

VMNAME (string)

ADMINUSERNAME (string)

ADMINPASSWORD (securestring)

OSTYPE (string)

VMSIZE (string)

GVMSIZE (string)
Standard_A1

UBUNTUOSVERSION (string)
14.04.2-LTS

FROMGATEWAYLOGIN (string)

ADDNAMETOCONCAT (string)

OK

3.2 The Parameters

You must specify the following parameters for your deployment.

Storage Account Name:

Specify the storage account name to use. This name has to be unique (so use your name or something else as a unique identifier). Also, only lower case letters and number are allowed. The name cannot have spaces, dashes or special characters.

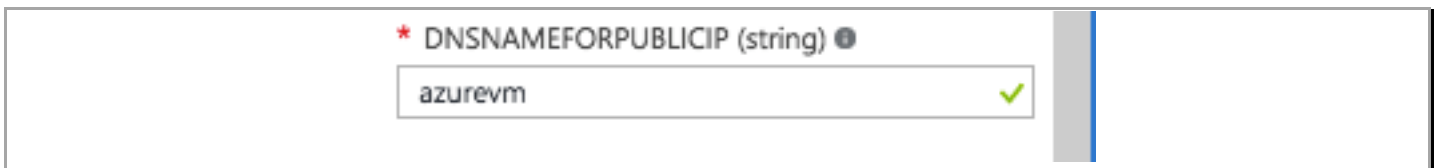


A screenshot of a deployment parameter field. The label is *** USERIMAGESTORAGEACCOUNTNAME (string)** with an information icon. The input box contains the text **azuretest** and has a green checkmark on the right. A vertical blue line is to the right of the input box.

Note: You must have a unique storage account name, for a successful deployment.

DNS Name for the VM-Series Firewall:

This is the DNS name for the VM-Series firewall (for management). It has to be unique name with lower case letters and numbers only. This name is used to address the firewall as opposed to its IP address.



A screenshot of a deployment parameter field. The label is *** DNSNAMEFORPUBLICIP (string)** with an information icon. The input box contains the text **azurevm** and has a green checkmark on the right. A vertical blue line is to the right of the input box.

DNS Name for the NAT VM:

This is the DNS name for the NAT instance. You can use this name in lieu of the IP address to connect to the NAT instance.



A screenshot of a deployment parameter field. The label is *** DNSNAMEFORPUBLICIPNAT (string)** with an information icon. The input box contains the text **azurenat** and has a green checkmark on the right. A vertical blue line is to the right of the input box.

VM Name:

The name for the VM-Series firewall in the firewall management dashboard



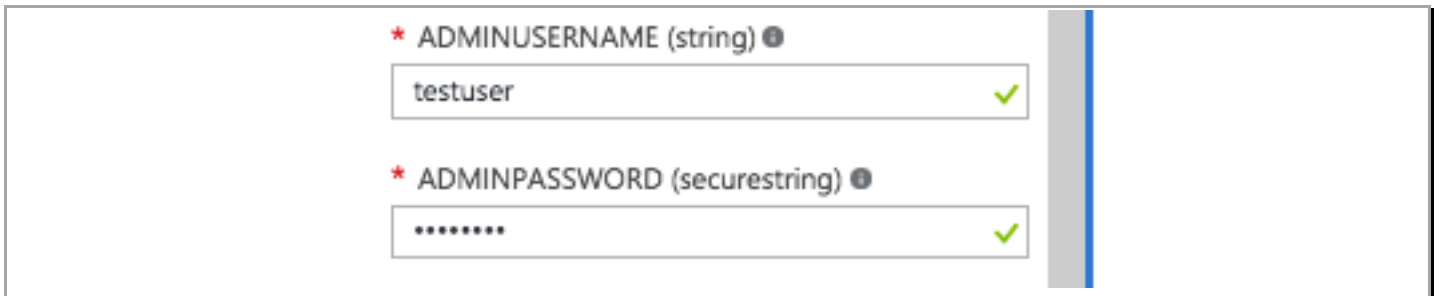
* VMNAME (string) ⓘ

azurengfw ✓

Username and password:

Specify the username and password for accessing the VM-Series firewall, the NAT VM, web and database servers. The supplied password must be between 6-72 characters long and must satisfy at least 3 of the following password complexity requirements:

- Contains an uppercase character.
- Contains a lowercase character.
- Contains a numeric digit.
- Contains a special character.



* ADMINUSERNAME (string) ⓘ

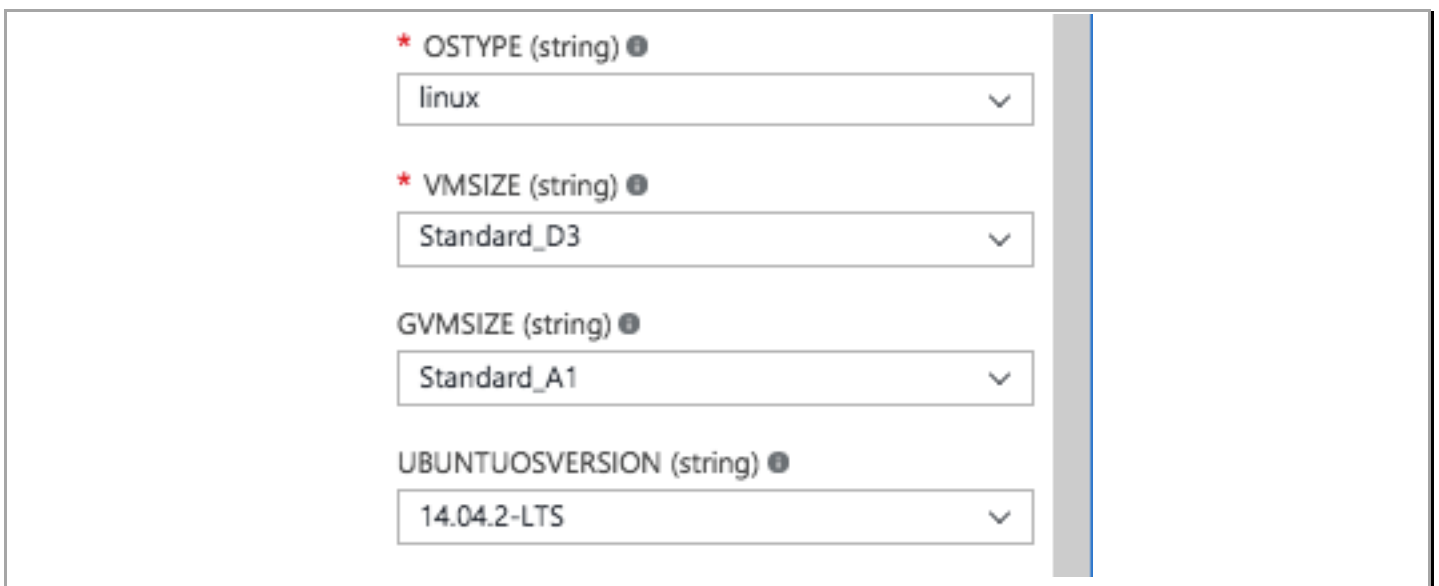
testuser ✓

* ADMINPASSWORD (securestring) ⓘ

***** ✓

Default Parameters:

Select the following parameters as shown in the screenshot below



* OSTYPE (string) ⓘ

linux ✓

* VMSIZE (string) ⓘ

Standard_D3 ✓

GVMSIZE (string) ⓘ

Standard_A1 ✓

UBUNTUOSVERSION (string) ⓘ

14.04.2-LTS ✓

Make sure the VM Size parameter is set to D3 and the GVM Size parameter is set to Standard_A1. These parameters indicate the VM sizes for the VM-Series firewall and the NAT VM respectively. The OS Type parameter specifies the type of OS (Linux in this case) for the VM-Series firewall and NAT VM instances. The Ubuntu OS version parameter specifies the version of Ubuntu to be used for the NAT VM.

From Gateway:

This parameter restricts the IP address from which you can access all of the resources within this VNET. As a best practice, specify an IP address (obtained from checkmyip.org) so the firewall and the NAT VM are not open to the world.

* FROMGATEWAYLOGIN (string) ⓘ

199.167.55.50 ✓

IP Address Prefix:

Specify the IP address prefix for the deployment. All subnets will begin with this prefix.

IPADDRESSPREFIX (string) ⓘ

10.5

Name to Concatenate:

Specify a string that to append to all the instances launched using this template. Allows one to identify one VM from another (in the case of multiple instances).

* ADDNAMETOCONCAT (string) ⓘ

azuretestdeploy ✓

Storage Account Type:

You can use the default storage account type or modify it to meet your needs.

STORAGEACCOUNTTYPE (string) ⓘ

Standard_LRS ▼

3.3 Review and Launch

After entering the parameters, select a subscription (an Azure pay-as-you-go subscription is recommended). Select “**+New**” for “Resource Group” and type in a resource group name. Select a region where the resources will be deployed and click on “**Review legal terms**”

	<div> <div>* Template</div> <div>Edit template</div> <div>></div> </div>
	<div> <div>* Parameters</div> <div>Edit parameters</div> <div>></div> </div>
	<div> <div>* Subscription</div> <div>Narayan-pay-as-you-go</div> <div>▼</div> </div>
	<div> <div>* Resource group</div> <div>+ New</div> <div>▼</div> </div>
	<div> <div>New resource group name</div> <div>azuretestrg</div> </div>
	<div> <div>* Resource group location</div> <div>East US</div> <div>▼</div> </div>
	<div> <div>* Legal terms</div> <div>Review legal terms</div> <div>></div> </div>

In the next tab, review the legal terms and click “**Accept**” or “**Create**”

* Template
Edit template >

* Parameters
Edit parameters >

* Subscription
Narayan-pay-as-you-go v

* Resource group
+ New v
New resource group name
azuretestrg ✓

* Resource group location
East US v

* Legal terms
Legal terms accepted >

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

The legal terms associated with any Marketplace offering may be found in the Azure portal. For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking "Create," I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; and (b) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s). Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

☐ Pin to dashboard

Create

Create

And finally, click **"Create"** on the left. This will deploy the template and create resources.

3.4 Check Deployment Status

If successfully deployed, select **Resource groups** to view the resource group that was created as part of the template, and under **"Last Deployment"** click **"Deploying"** to view all the resources that are being created.

Palo Alto Networks Azure ARM Template Deployment Guide

The screenshot displays the Microsoft Azure portal interface. The breadcrumb navigation at the top indicates the path: **Resource groups** > **narayantestazurerg** > **Deployment history** > **Microsoft.Template**.

The left sidebar contains the navigation menu with options: **New**, **Resource groups**, **All resources**, **Recent**, **App Services**, **Virtual machines (classic)**, **Virtual machines**, and **SQL databases**.

The main content area is divided into two panes. The left pane, titled **Resource groups** (Palo Alto Networks), includes a filter bar with the text "Filter items..." and a dropdown menu showing "Narayan-pay-as-you-go". Below this is a table with the following data:

NAME
narayantestazurerg ...

The right pane, titled **narayantestazurerg** (Resource group), contains an **Essentials** section with the following details:

Subscription name	Subscription ID
Narayan-pay-as-you-go	0f3ba96c-a3c7-4eac-b599-ed9882801672
Last deployment	Location
3/31/2016 (Deploying)	West US

Below the Essentials section is a **Summary** section with an **Add tiles** (+) button. The **Resources** tile is expanded, showing a list of resources:

Resource Name
DBeth0
eth0
eth1
eth2
NATeth0
Webeth0
DefaultNSG
fwPublicIP
natPublicIP

At the bottom of the Summary section is an **Add a section** (+) button.

3.4.1 Deployment failed

If the deployment is unsuccessful, the deployment status will change from **Deploying** to **Failed**

Essentials ^

Subscription name
Narayan-pay-as-you-go

Last deployment
3/31/2016 (Failed)

Subscription ID
0f3ba96c-a3c7-4eac-b599-ed9882801672

Location
West US

All settings →

To debug the root cause, click the **Failed** link and select **Audit Logs** in the next tile.

Filter settings

SUPPORT + TROUBLESHOOTING

Audit logs >

GENERAL

Properties >

Resources >

Resource costs >

Deployments >

Alerts >

Export template >

RESOURCE MANAGEMENT

Users >

Tags >

Filtered for past week by resource group azuretestrg event category = All, levels = All

2

1.8

1.6

1.4

1.2

1

0.8

0.6

0.4

0.2

0

12:14 PM

12:15 PM

12:16 PM

12:17 PM

CRITICAL

ERROR

WARNING

INFORMATIONAL

0

2

0

1

Filter items ...

OPERATION ^

LEVEL ^

STATUS ^

RESOURCE ^

TL... ^

Validate

Error

Failed

...deployments/Mic...

Just no...

Validate

Error

Failed

...deployments/Mic...

4 min ...

Update resource gr...

Informational

Succeeded

...azuretestrg

4 min ...

LEVEL

Error

STATUS

Failed

TIME

Thursday, March 31, 2016, 12:17:38 PM

CALLER

niyengar@paloaltonetworks.com

CORRELATION IDS

34b7f647-ed67-43e3-b9ac-8c9e74a8533c

EVENT

LEVEL

STATUS

TIME

microsoft.resources/depl...

Error

Failed

4 m...

microsoft.resources/depl...

Informational

Started

4 m...




Then, click on the error(s) reported to get details on the failure reason.

Palo Alto Networks Azure ARM Template Deployment Guide

LEVEL	Error	OPERATION NAME	microsoft.resources/deployments/validate/action
STATUS	Failed	STATUS	Failed
TIME	Thursday, March 31, 2016, 12:17:38 PM	EVENT TIMESTAMP	Thu Mar 31 2016 12:17:38 GMT-0700 (PDT)
CALLER	niyengar@paloaltonetworks.com	UTC TIMESTAMP	Thu, 31 Mar 2016 19:17:38 GMT
CORRELATION IDS	34b7f647-ed67-43e3-b9ac-8c9e74a8533c	CALLER	niyengar@paloaltonetworks.com
AUTHORIZATION		AUTHORIZATION	action:microsoft.resources/deployments/validate/action role:scope/subscriptions/0f3ba96c-a3c7-4eac-b599-ed9882801672/resourcegroups/azuretestrg/providers/microsoft.resources/deployments/Microsoft.Template
RESOURCE URI		RESOURCE URI	/subscriptions/0f3ba96c-a3c7-4eac-b599-ed9882801672/resourcegroups/azuretestrg/providers/microsoft.resources/deployments/Microsoft.Template
SUBSCRIPTION ID		SUBSCRIPTION ID	0f3ba96c-a3c7-4eac-b599-ed9882801672
EVENT SUBMISSION TIMESTAMP		EVENT SUBMISSION TIMESTAMP	Thu Mar 31 2016 12:17:51 GMT-0700 (PDT)
OPERATION ID		OPERATION ID	34b7f647-ed67-43e3-b9ac-8c9e74a8533c
SUBSTATUS		SUBSTATUS	Bad Request (HTTP Status Code: 400)
CORRELATION ID		CORRELATION ID	34b7f647-ed67-43e3-b9ac-8c9e74a8533c
HTTP REQUEST		HTTP REQUEST	clientRequestId:c5d82fc1-f6f4-4b04-8e39-53be2ae7e021 clientIpAddress:199.167.55.50 method:POST
LEVEL	Error	LEVEL	Error
RESOURCE GROUP	azuretestrg	RESOURCE GROUP	azuretestrg
RESOURCE PROVIDER	Microsoft Resources	RESOURCE PROVIDER	Microsoft Resources
CATEGORY	Administrative	CATEGORY	Administrative
PROPERTIES		PROPERTIES	statusCode:BadRequest serviceRequestId:statusMessage:{"error":{"code":"InvalidTemplateDeployment","message":"The template deployment 'Microsoft.Template' is not valid according to the validation procedure. The tracking id is '34b7f647-ed67-43e3-b9ac-8c9e74a8533c'. See inner errors for details. Please see http://aka.ms/arm-deploy for usage details."},"details":[{"code":"QuotaExceeded","message":"Operation results in exceeding quota limits of Core. Maximum allowed: 10, Current in use: 0, Additional requested: 11."}]}

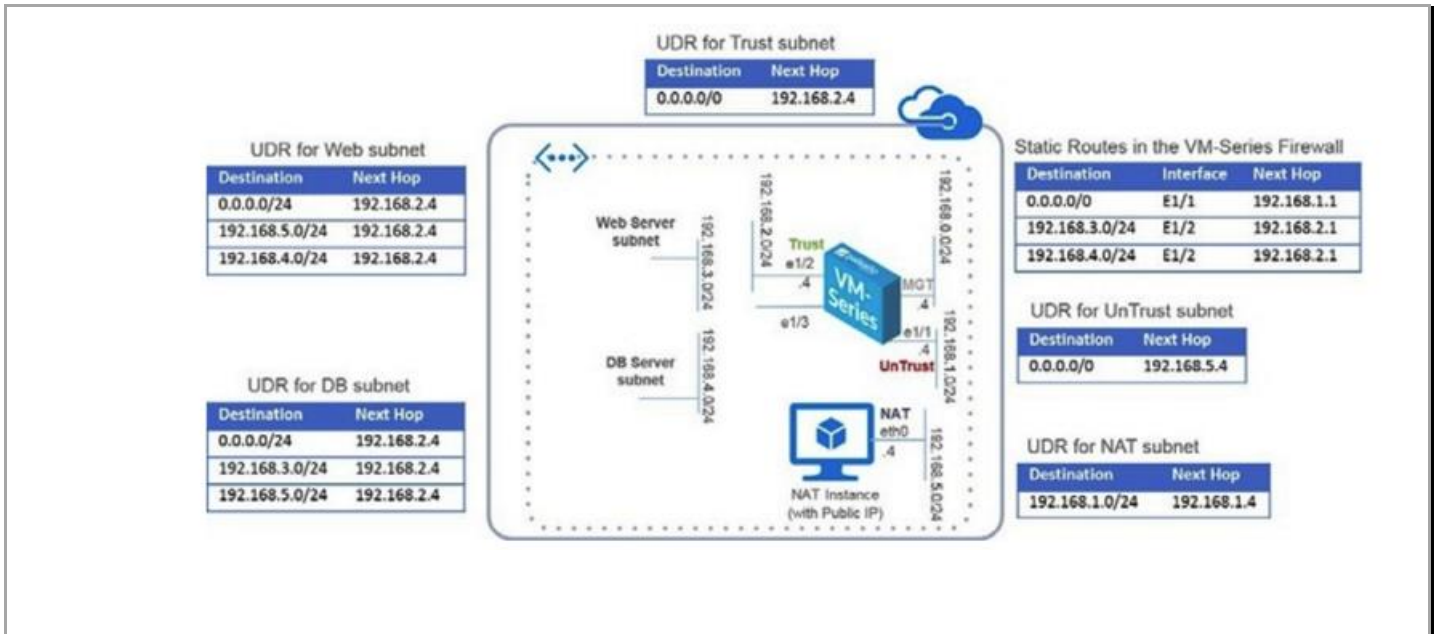
3.4.2 Deployment successful

If the ARM template deployment was successful, the deployment state will show as “**Succeeded**”

Essentials ^	  
Subscription name Narayan-pay-as-you-go	Subscription ID 0f3ba96c-a3c7-4eac-b599-ed9882801672
Last deployment 3/31/2016 (Succeeded)	Location West US
All settings →	

4. Review the Provisioned Resources

Verify that the resources match this topology. If you customized the template, the subnets may be different.







Here is a high level break down:

DB server, NAT instance, VM-Series firewall and web server respectively.

	DB-testazure	Virtual machine	azuretestnarayanrg	West US	Narayan-pay-as-you... ..
	natInstance-testazure	Virtual machine	azuretestnarayanrg	West US	Narayan-pay-as-you... ..
	pan-vm-series-testazure	Virtual machine	azuretestnarayanrg	West US	Narayan-pay-as-you... ..
	Websever-testazure	Virtual machine	azuretestnarayanrg	West US	Narayan-pay-as-you... ..


Network interfaces

For the firewall: eth0 is the management interface, eth1 is in the untrust zone and eth2 is in the trust zone.

	DBeth0	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
	eth0	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
	eth1	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
	eth2	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
	NATeth0	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
	Webeth0	Network interf...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...

The DefaultNSG (network security group)

This security group applies to the Azure Resource Group as a whole. The network security group specifies rules that allow or deny access to the resources within the resource group and provides a very rudimentary port/protocol based firewall.






	DefaultNSG	Network secur...	azuretestnarayanrg	West US	Narayan-pay-as-you...	...
---	------------	------------------	--------------------	---------	-----------------------	-----

Inbound and outbound rules for the DefaultNSG

Inbound security rules						
DefaultNSG						
<div> <div>+</div> Add <div>Default rules</div> </div>						
<div> <div>Search inbound security rules</div> </div>						
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
100	Allow-Outside-From-IP	199.167.55.50/32	Any	Any/Any	Allow	...
101	Allow-Intra	10.5.0.0/16	Any	Any/Any	Allow	...
200	Default-Deny	Any	Any	Any/Any	Deny	...
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	Any/Any	Allow	...
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	Any	Any/Any	Allow	...
65500	DenyAllInBound	Any	Any	Any/Any	Deny	...

Outbound security rules						
DefaultNSG						
<div> <div>+</div> Add <div>Default rules</div> </div>						
<div> <div>Search outbound security rules</div> </div>						
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
65000	AllowVnetOutBound	VirtualNetwork	VirtualNetwork	Any/Any	Allow	...
65001	AllowInternetOutBound	Any	Internet	Any/Any	Allow	...
65500	DenyAllOutBound	Any	Any	Any/Any	Deny	...

User defined Routes (UDRs)

 DB-to-FW	Route table	azuretestnaraynrg	West US	Narayan-pay-as-you... ...
 FWUntrust-to-NAT	Route table	azuretestnaraynrg	West US	Narayan-pay-as-you... ...
 NAT-to-FW	Route table	azuretestnaraynrg	West US	Narayan-pay-as-you... ...
 Trust-to-intranetwork	Route table	azuretestnaraynrg	West US	Narayan-pay-as-you... ...
 Web-to-FW	Route table	azuretestnaraynrg	West US	Narayan-pay-as-you... ...

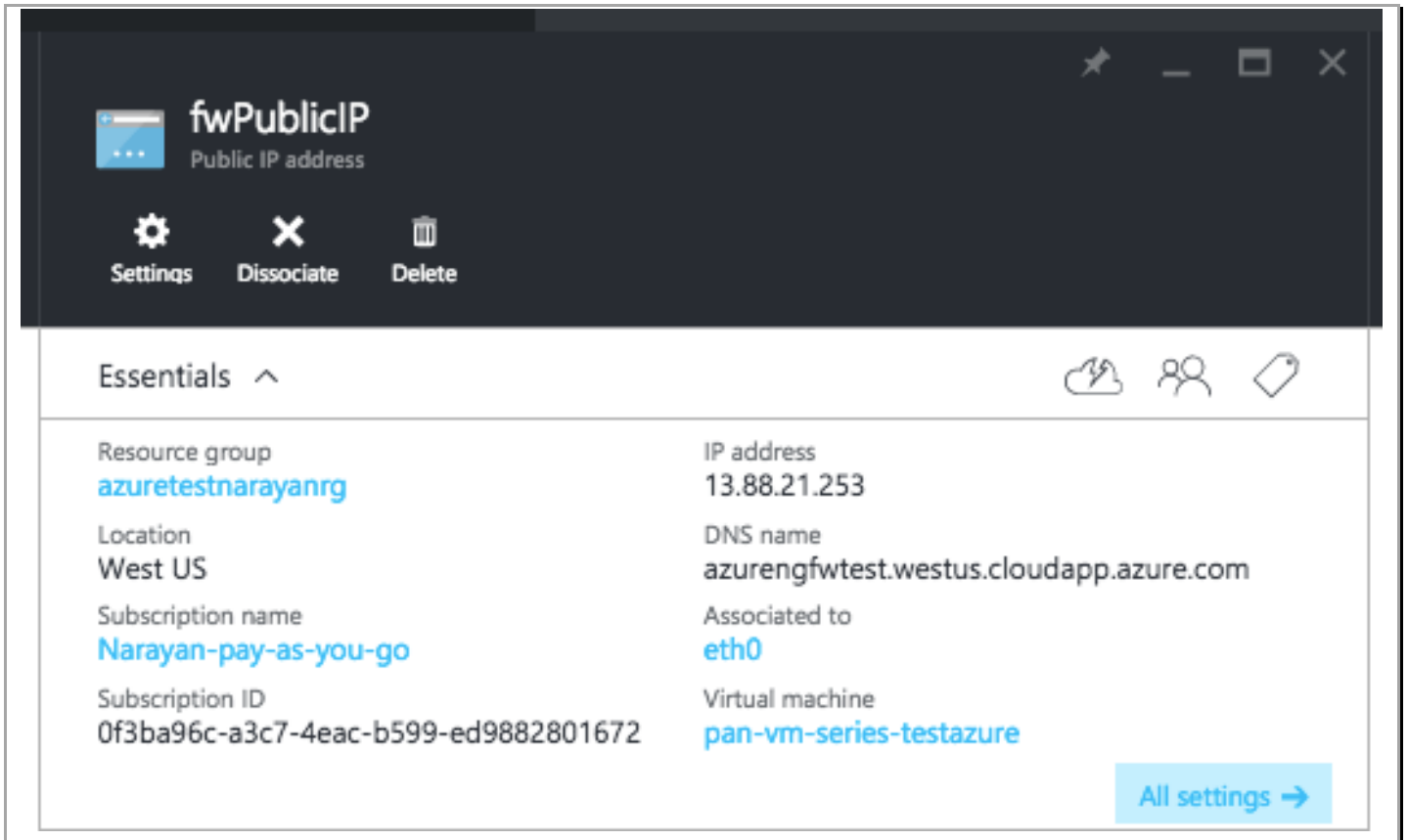
The above UDRs enable the VM-Series firewall to secure the Azure resource group. For the five subnets—Trust, Untrust, Web, DB, and NAT—included in the template, you have five route tables, one for each subnet with user defined rules for routing traffic to the VM-Series firewall and the NAT virtual machine.

Public IPs

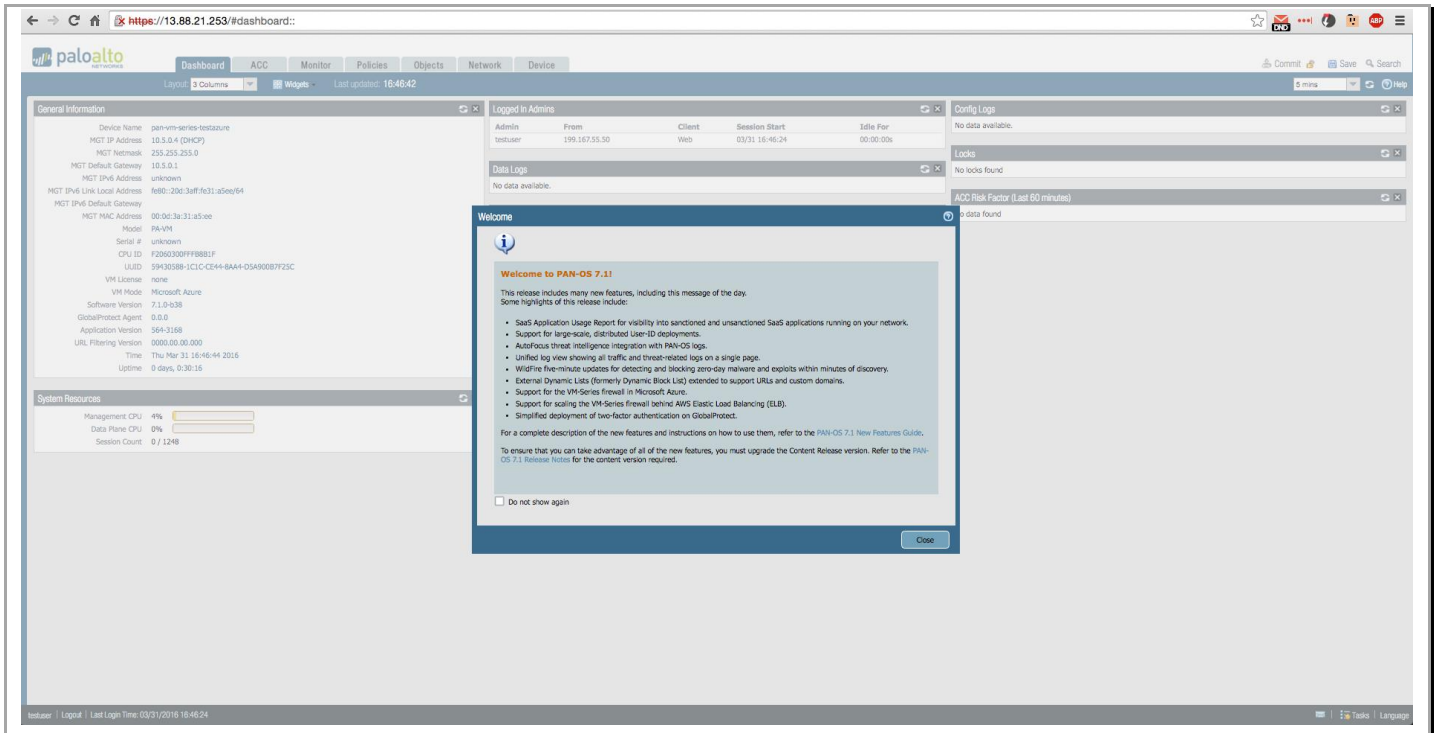
 fwPublicIP	Public IP addre...	azuretestnaraynrg	West US	Narayan-pay-as-you... ...
 natPublicIP	Public IP addre...	azuretestnaraynrg	West US	Narayan-pay-as-you... ...

5. Configure the VM-Series Firewall

Use the public IP address or the DNS name, and the username and password you specified to log in to the firewall.



Palo Alto Networks Azure ARM Template Deployment Guide



Please refer to the PAN OS 7.1 admin guide <
<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os.html>>

and the Configuring VM-Series on Azure guide

< <https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/set-up-the-vm-series-firewall-in-azure.html>> on how to configure the firewall, add routes and secure traffic.

6. Cleanup

If done, delete the resource group in order to cleanup and remove all the resources created.

The screenshot shows the Azure portal interface for deleting a resource group. The left sidebar shows 'Resource groups' with a search filter 'Narayan-pay-as-you-go'. The top bar shows the 'Delete' button for the 'narayantestazurg' resource group. The main area displays a warning dialog: 'Are you sure you want to delete "narayantestazurg"?'. The dialog includes a warning icon and text: 'Warning! Deleting the "narayantestazurg" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.' Below the warning, there is a text input field for the resource group name, which is pre-filled with 'narayantestazurg'. To the right of the dialog, a table titled 'Affected resources' lists the resources that will be deleted. The table has columns: NAME, TYPE, RESOURCE GROU..., LOCATION, and SUBSCRIPTI. The resources listed are: DBeth0, eth0, eth1, eth2, NATeth0, Webeth0, DefaultNSG, fwPublicIP, natPublicIP, DB-to-FW, FWUnst-to-NAT, NAT-to-FW, and Intra-to-Intranetwork. At the bottom of the dialog, there are 'Delete' and 'Cancel' buttons.

NAME	TYPE	RESOURCE GROU...	LOCATION	SUBSCRIPTI
DBeth0	Network L...	narayantestazu...	West US	Narayan-
eth0	Network L...	narayantestazu...	West US	Narayan-
eth1	Network L...	narayantestazu...	West US	Narayan-
eth2	Network L...	narayantestazu...	West US	Narayan-
NATeth0	Network L...	narayantestazu...	West US	Narayan-
Webeth0	Network L...	narayantestazu...	West US	Narayan-
DefaultNSG	Network s...	narayantestazu...	West US	Narayan-
fwPublicIP	Public IP a...	narayantestazu...	West US	Narayan-
natPublicIP	Public IP a...	narayantestazu...	West US	Narayan-
DB-to-FW	Route table	narayantestazu...	West US	Narayan-
FWUnst-to-NAT	Route table	narayantestazu...	West US	Narayan-
NAT-to-FW	Route table	narayantestazu...	West US	Narayan-
Intra-to-Intranetwork	Route table	narayantestazu...	West US	Narayan-