VM-Series for Azure

Azure Two-Tier ARM Template Deployment Guide

http://www.paloaltonetworks.com

May, 2016

Table of Contents

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:

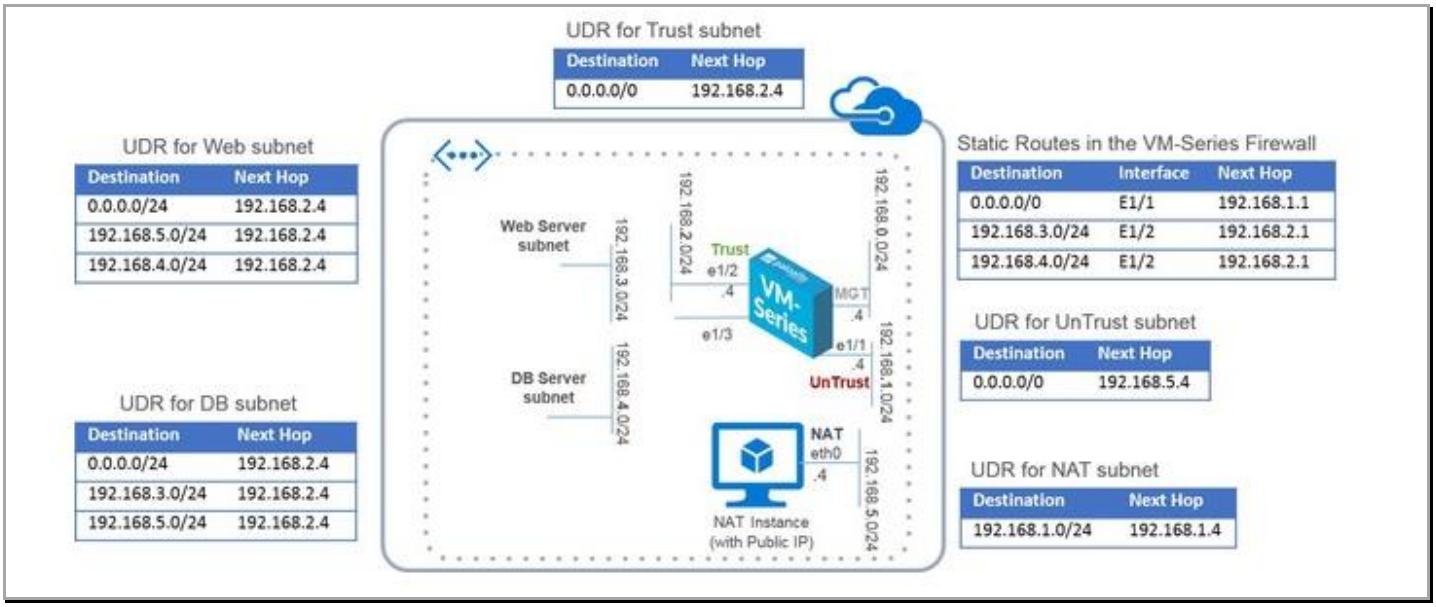


Figure 1: Template topology

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

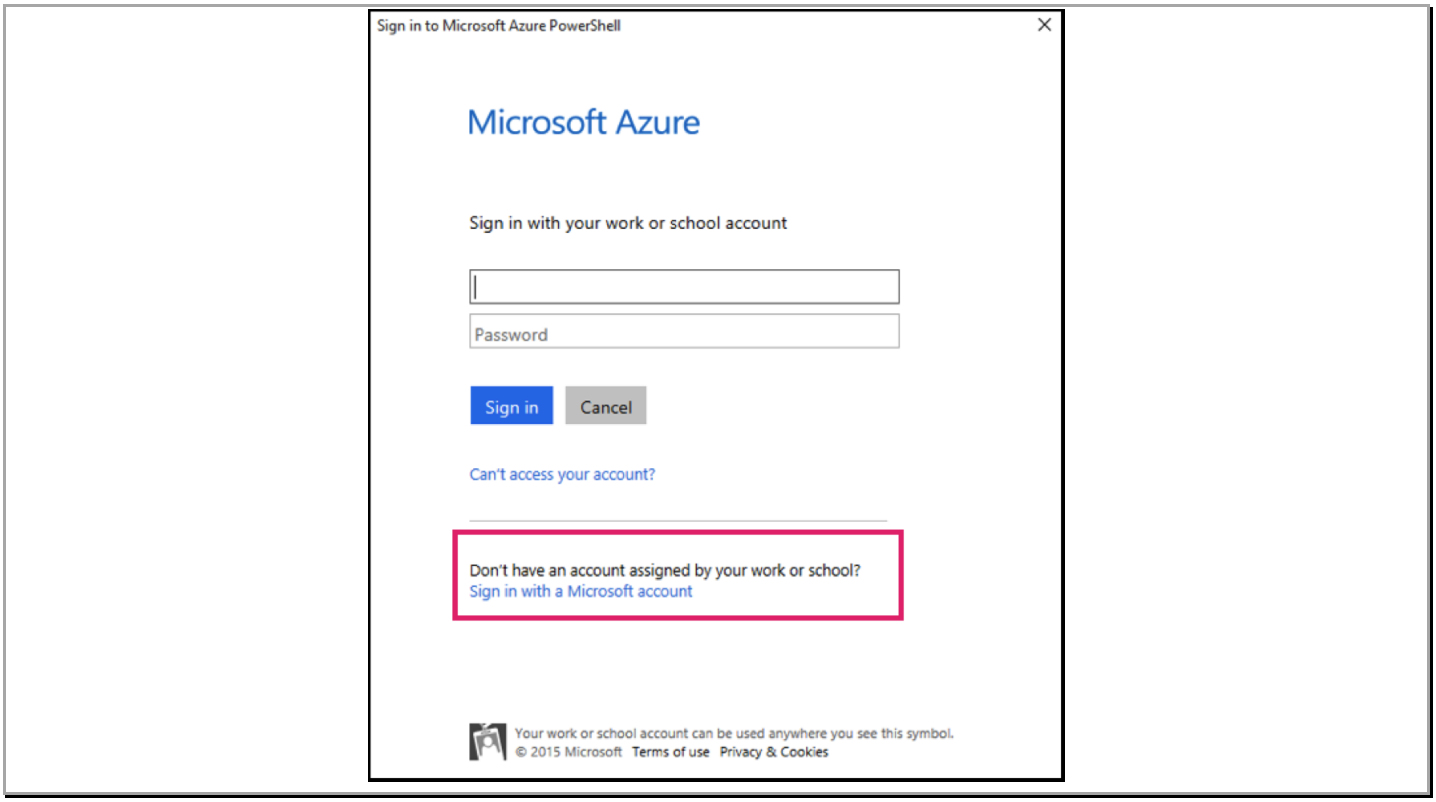
2. Prerequisites

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".



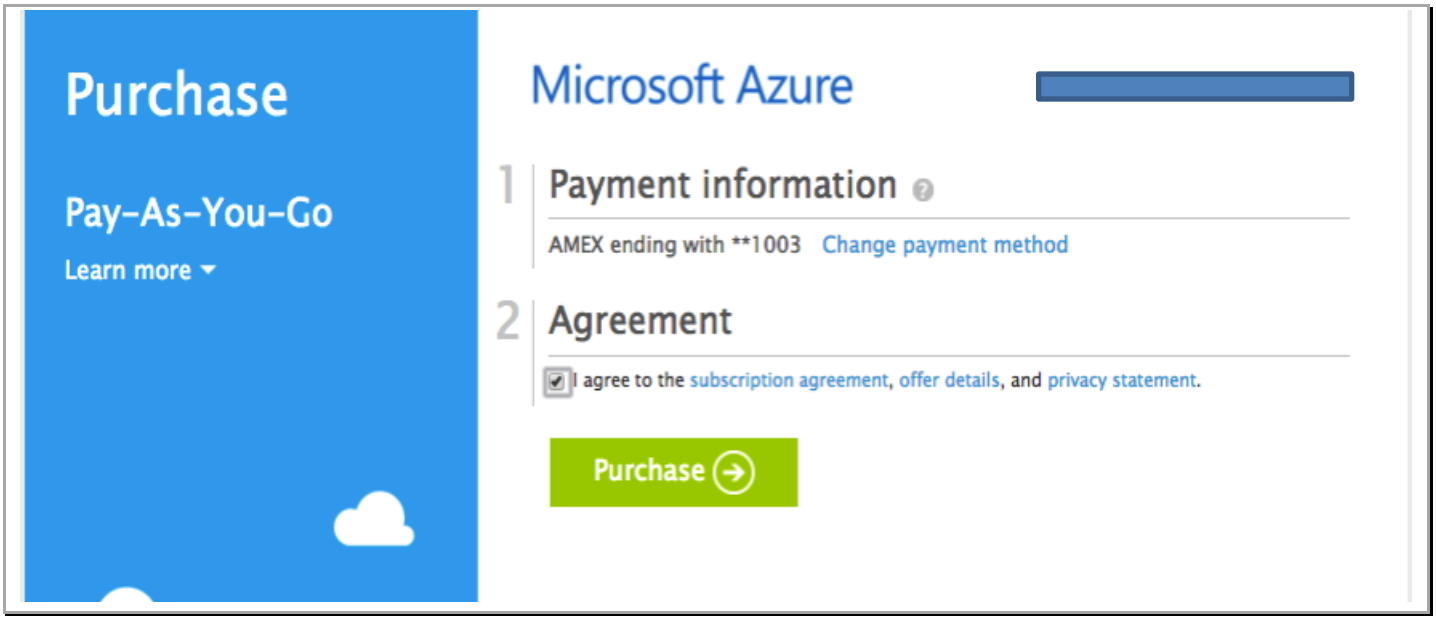
The free trial expires 30 days from account creation date or when $200 free credits are used up.

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**"

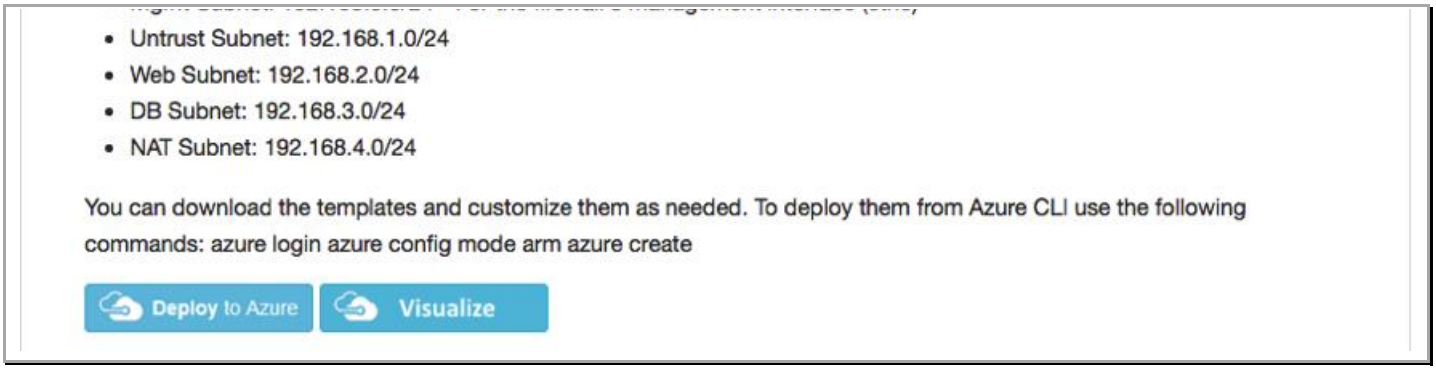


3. Launch The ARM Template

3.1 Deploy from github

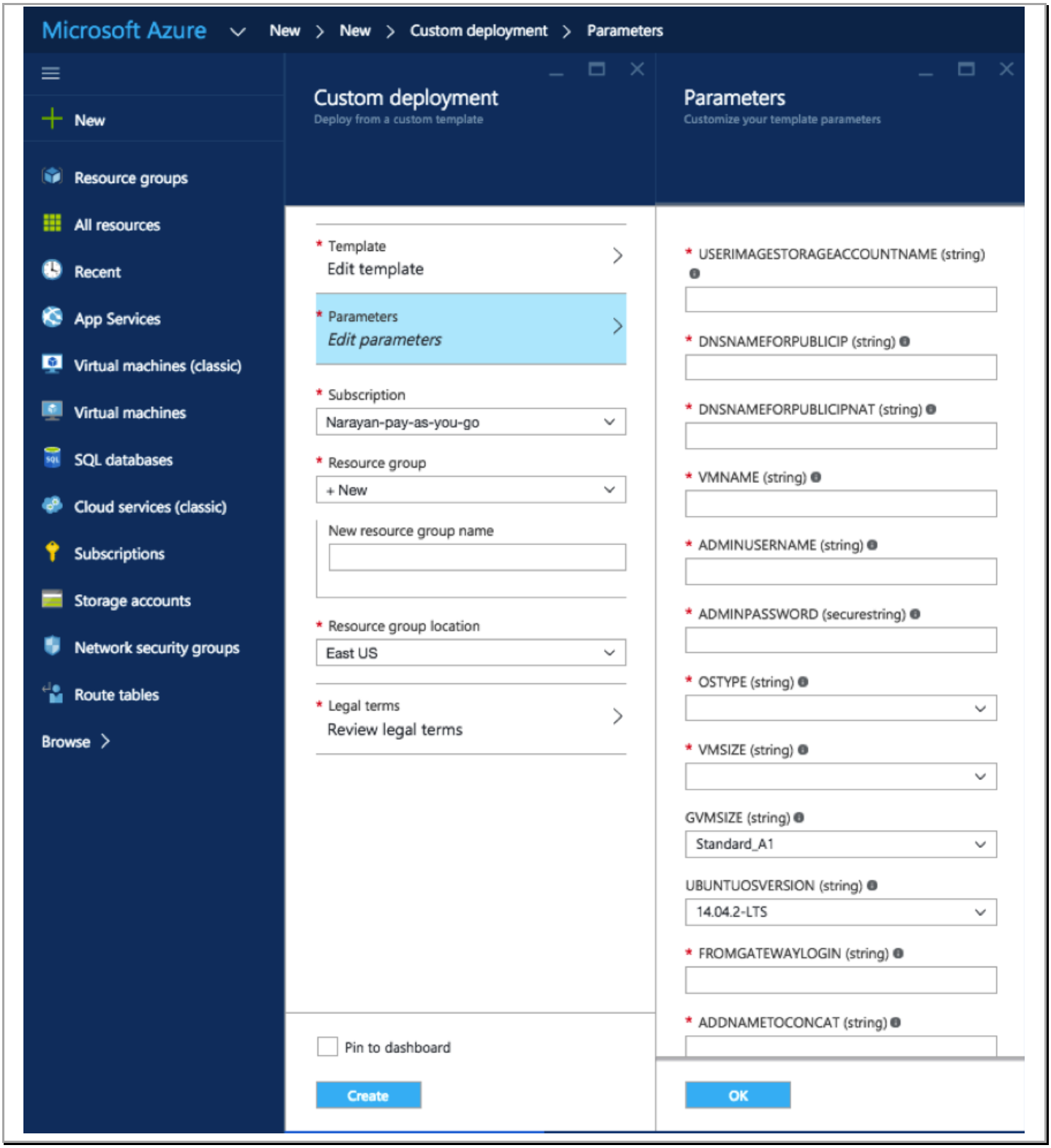
This document covers how to launch the template from the Azure portal. For details on using the Azure command line please refer to following doc
https://www.paloaltonetworks.com/documentation/71/virtualization/virtualization/set-up-the-vm-series-firewall-in-azure/use-the-arm-template-to-deploy-the-vm-series-firewall

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.

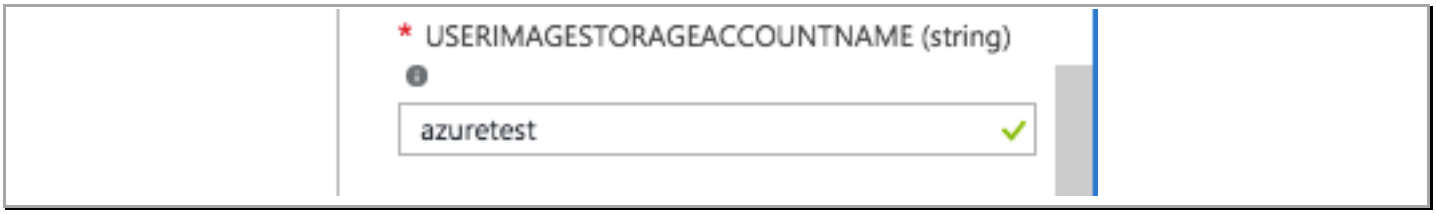
Click “**Deploy to Azure**” link. You will be prompted to log in to your Azure account and prompted to specify some template parameters.



3.2 The Parameters

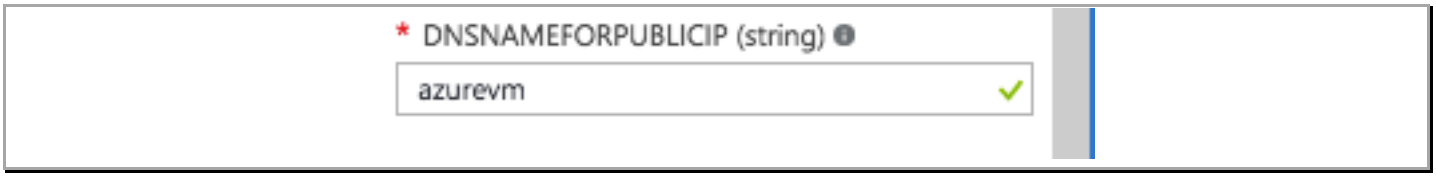
You must specify the following parameters for your deployment.

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.



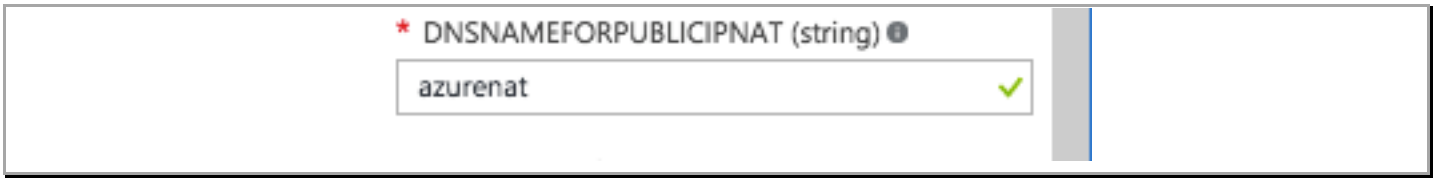
Note: You must have a unique storage account name, for a successful deployment.

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.



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.



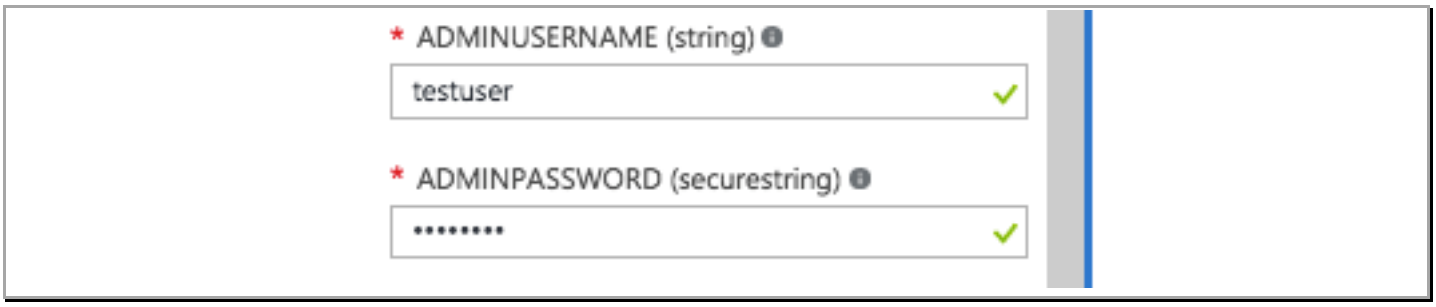
VM Name:

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

Username and password:

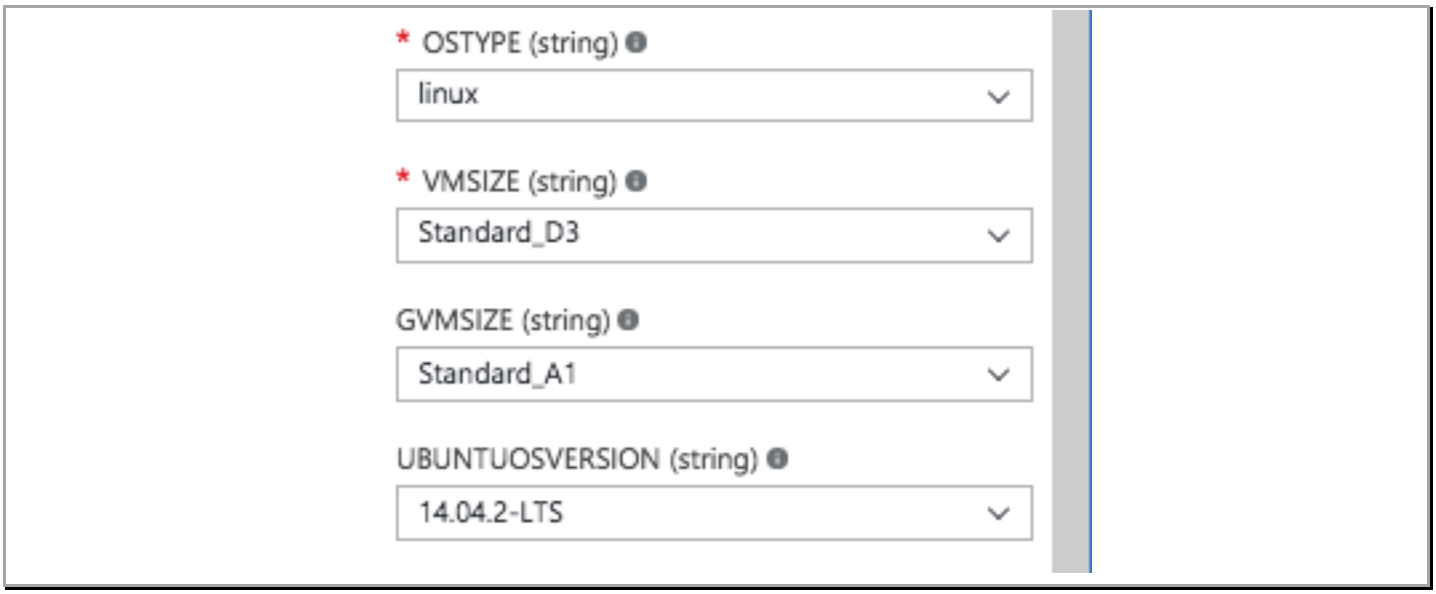
Specify the username and password for accessing the VM-Series firewall, the NAT VM, web and database servers. The supplied password must be between 6-72 characters long and must satisfy at least 3 of the following password complexity requirements:

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



Default Parameters:

Select the following parameters as shown in the screenshot below



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:

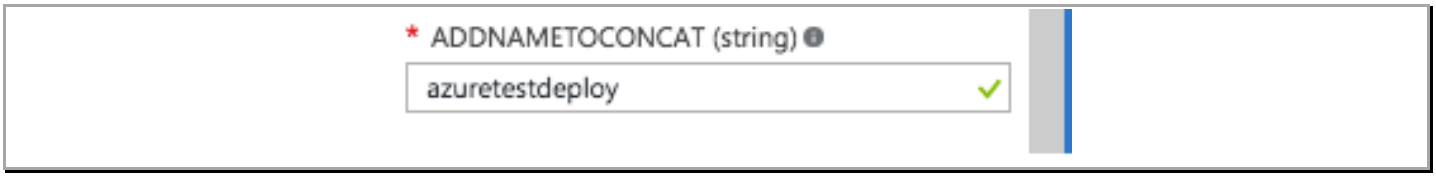
This parameter restricts the IP address from which you can access all of the resources within this VNET. As a best practice, specify an IP address (obtained from checkmyip.org) so the firewall and the NAT VM are not open to the world.

IP Address Prefix:

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

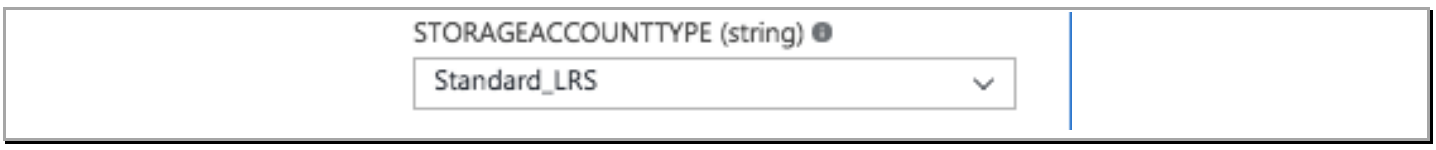
Name to Concatenate:

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).



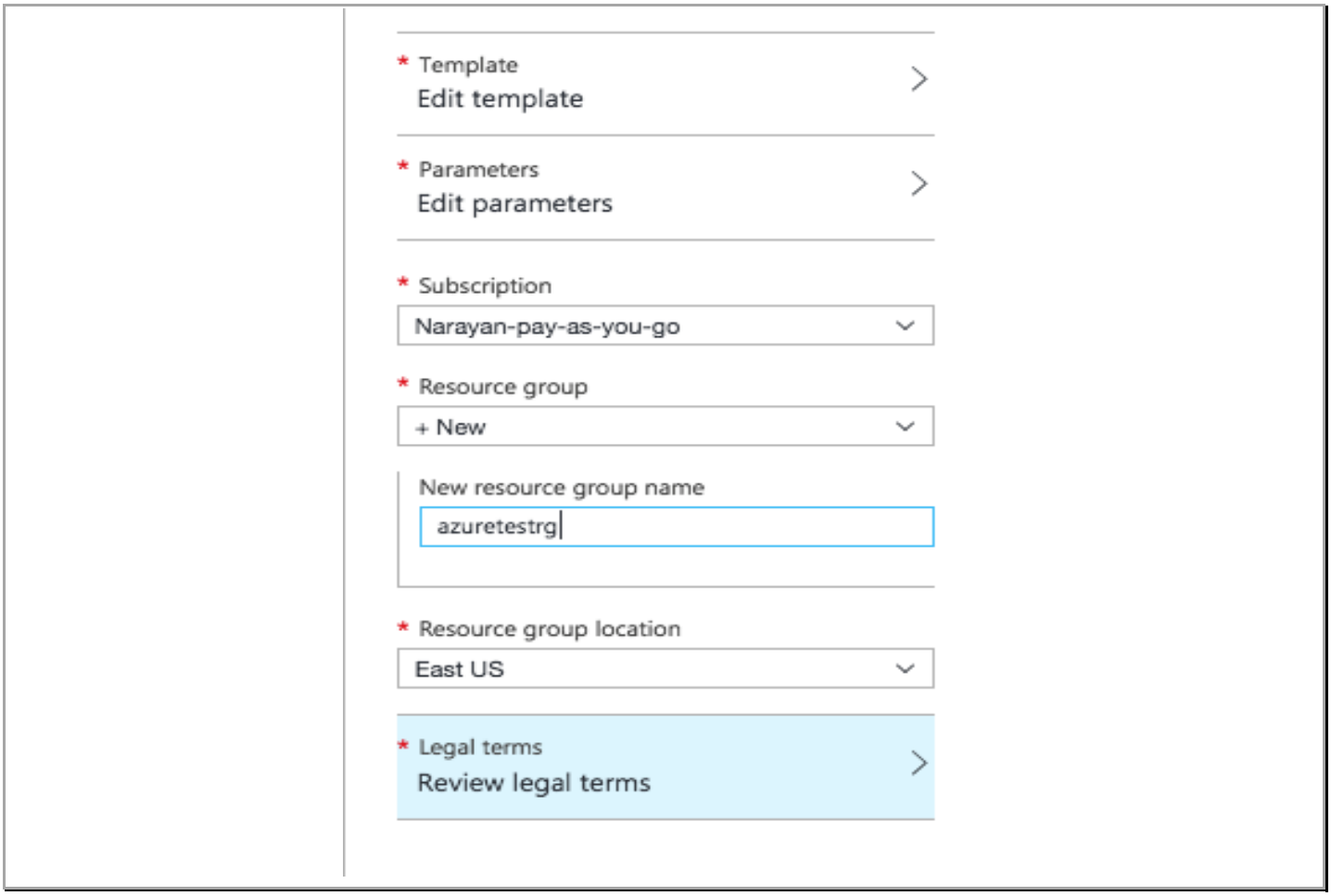
Storage Account Type:

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

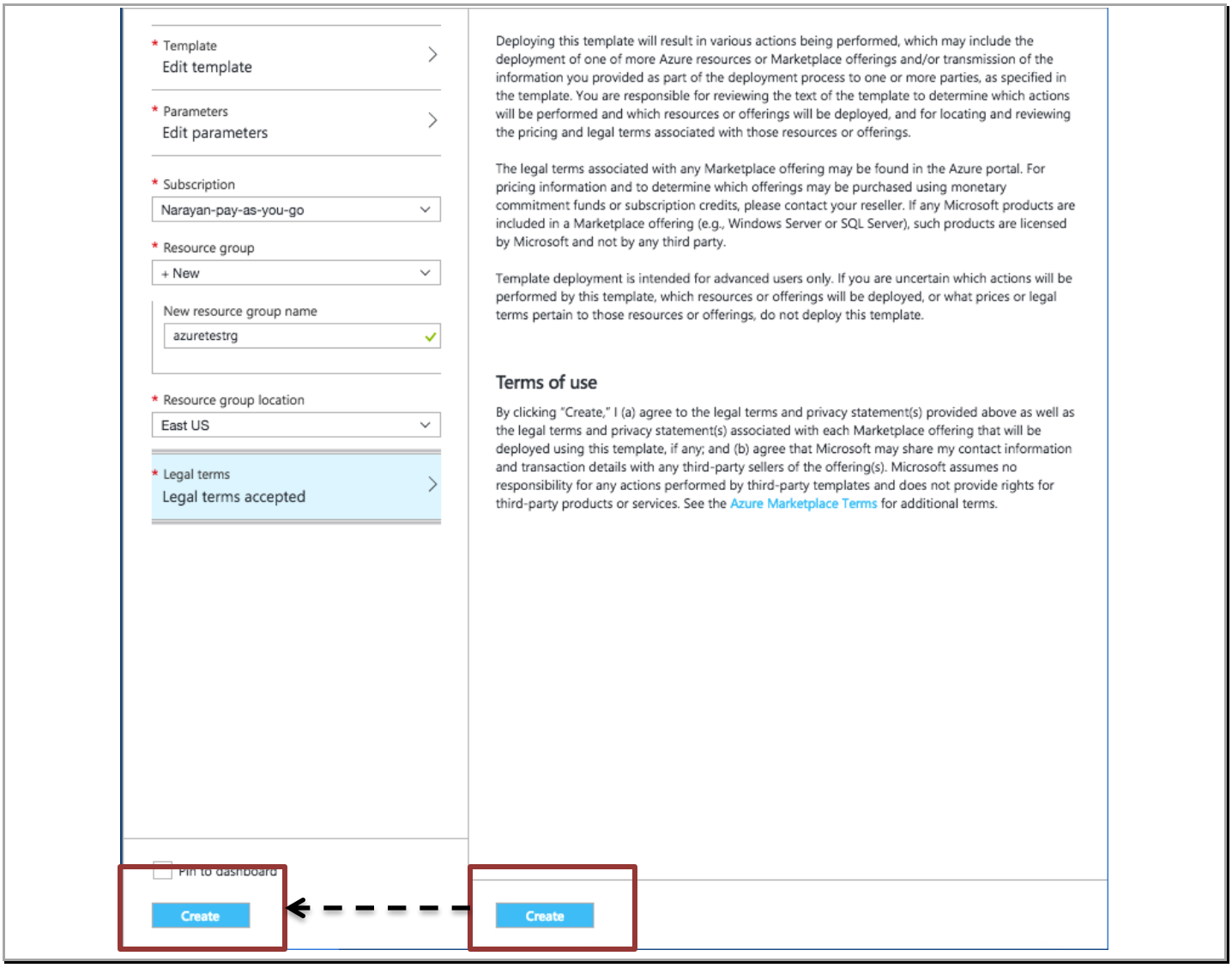


3.3 Review and Launch

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**"



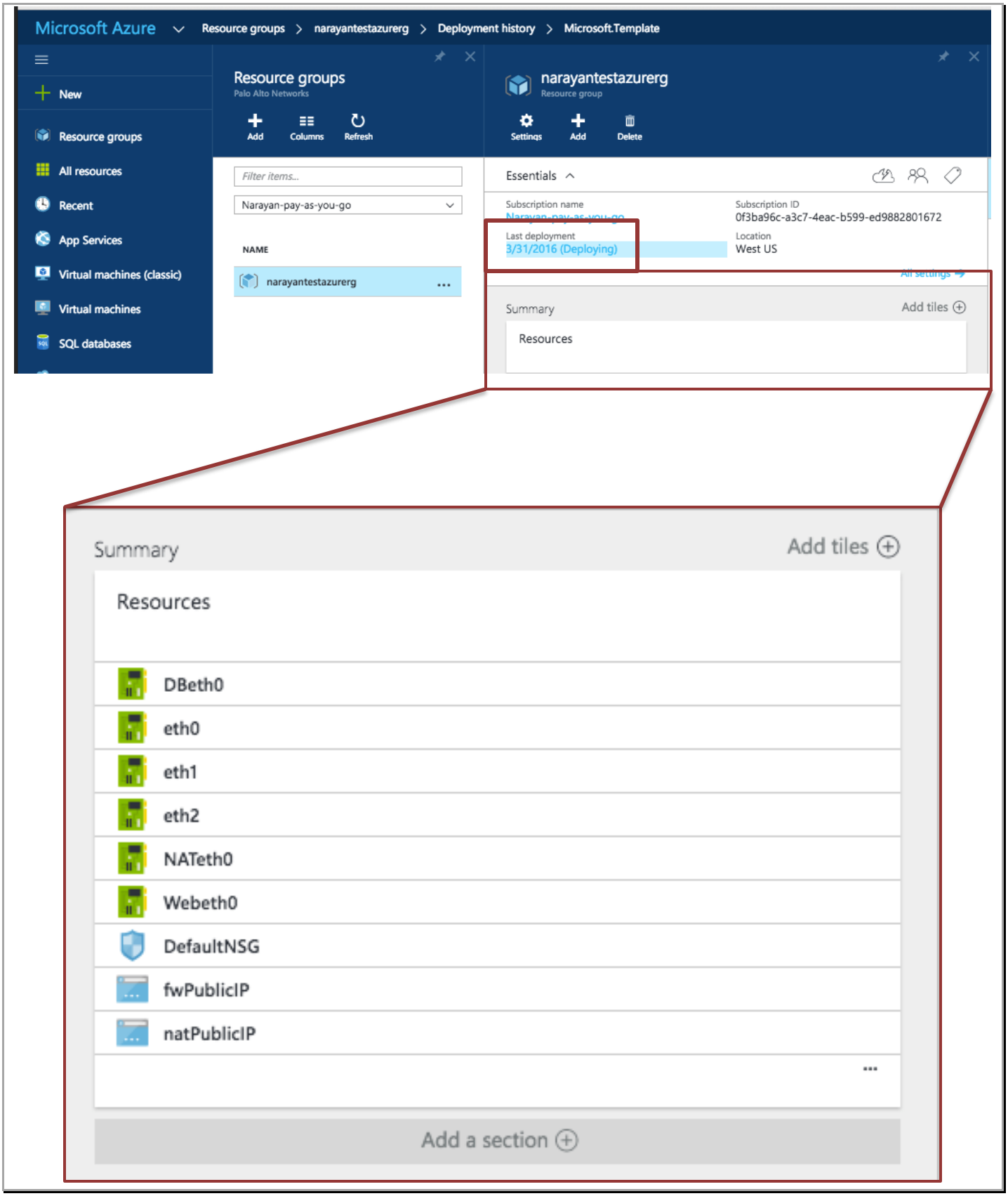
In the next tab, review the legal terms and click "**Accept**" or "**Create**"



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.

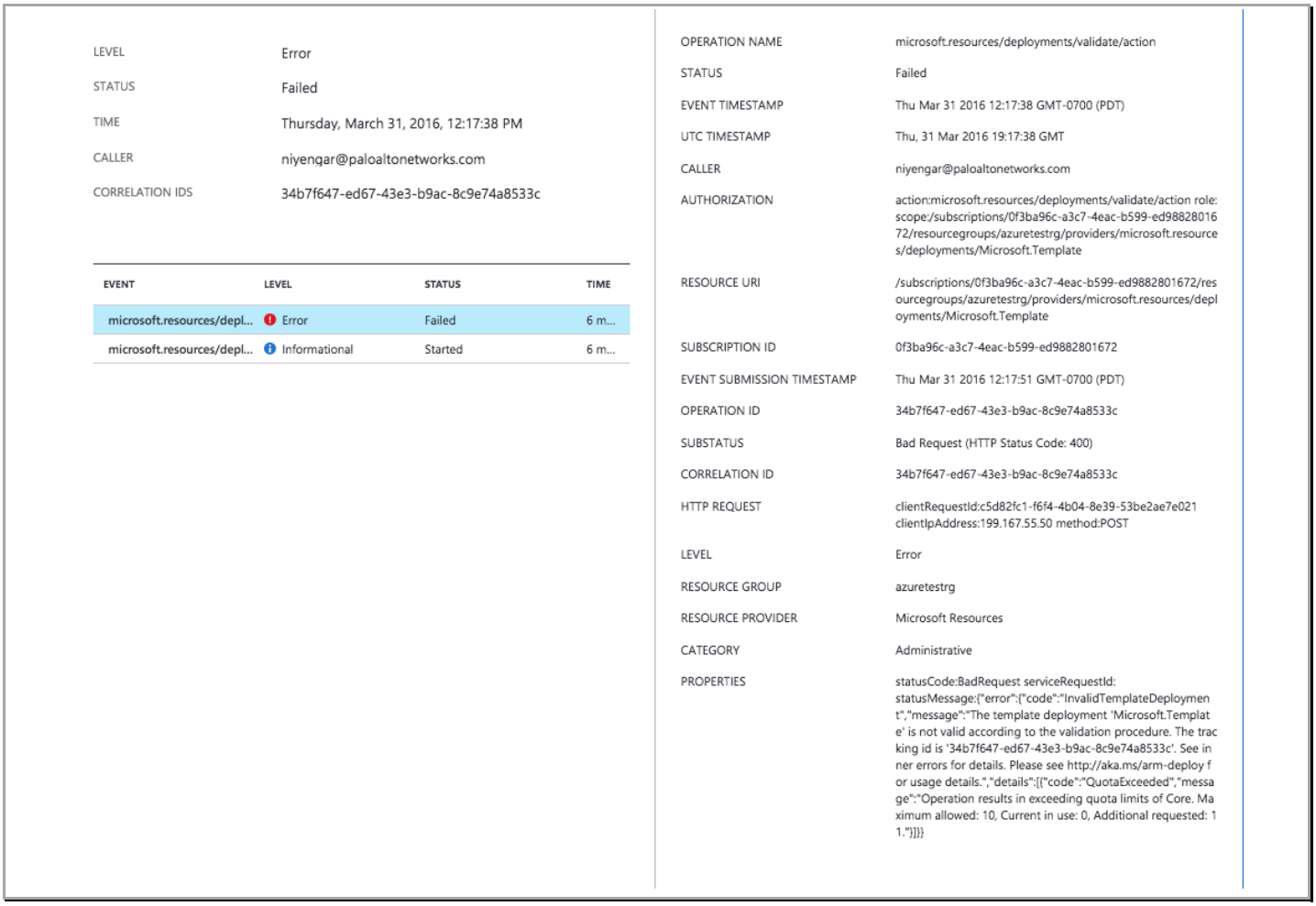

Microsoft Azure
Resource groups
narayantestazurerg
Deployment history
Microsoft.Template
New
Resource groups
All resources
Recent
App Services
Virtual machines (classic)
Virtual machines
SQL databases
Resource groups
Palo Alto Networks
Add
Columns
Refresh
Filter items...
Narayan-pay-as-you-go
NAME
narayantestazurerg
narayantestazurerg
Resource group
Settings
Add
Delete
Essentials
Subscription name
Subscription ID
0f3ba96c-a3c7-4eac-b599-ed9882801672
Last deployment
3/31/2016 (Deploying)
Location
West US
Summary
Add tiles
Resources
Summary
Add tiles
Resources
DBeth0
eth0
eth1
eth2
NATeth0
Webeth0
DefaultNSG
fwPublicIP
natPublicIP
Add a section

3.4.1 Deployment failed

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

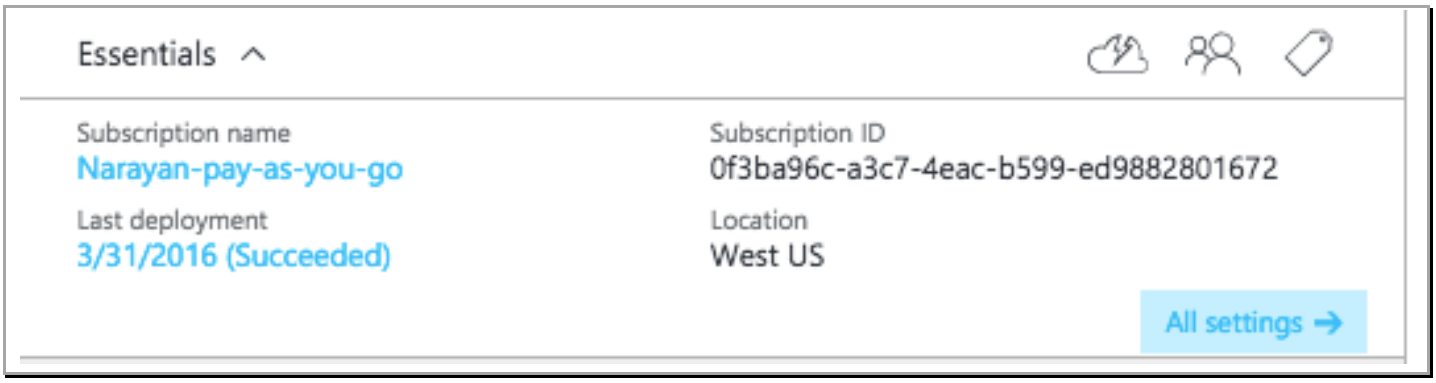
To debug the root cause, click the "**Failed**" link and select "**Audit Logs**" in the next tile.

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



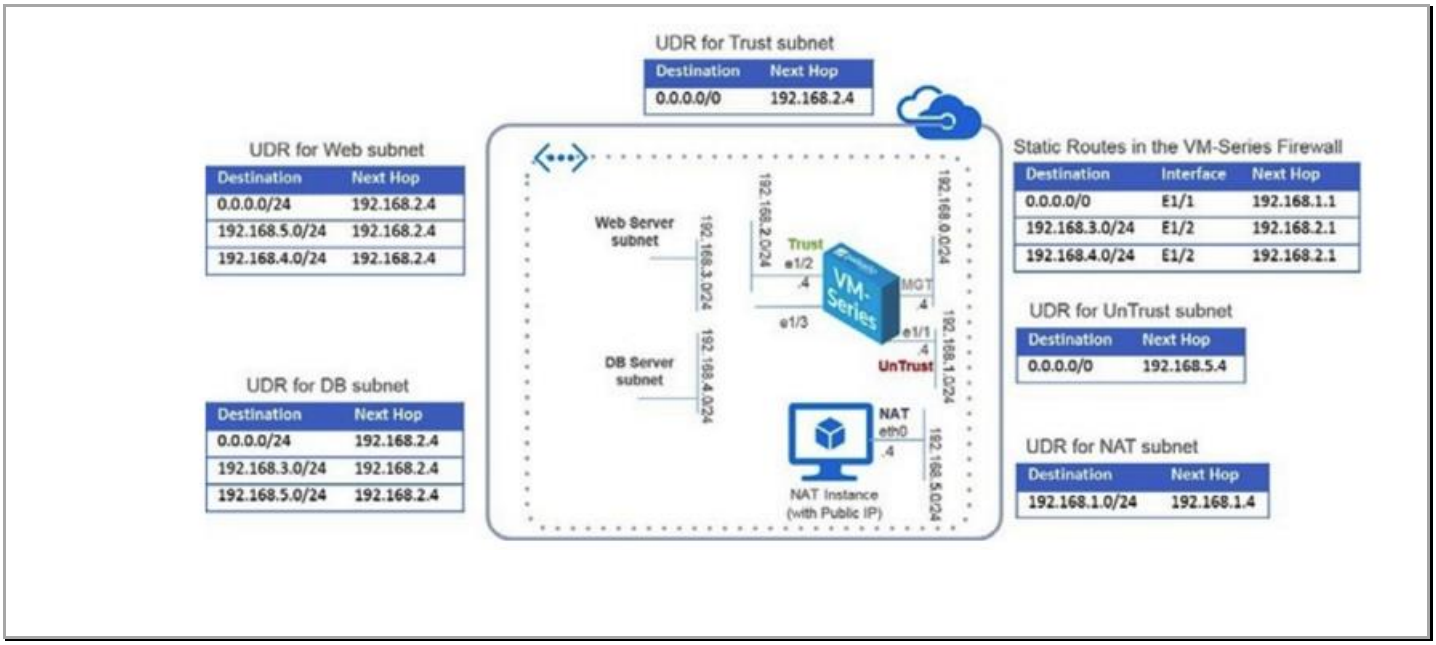
3.4.2 Deployment successful

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



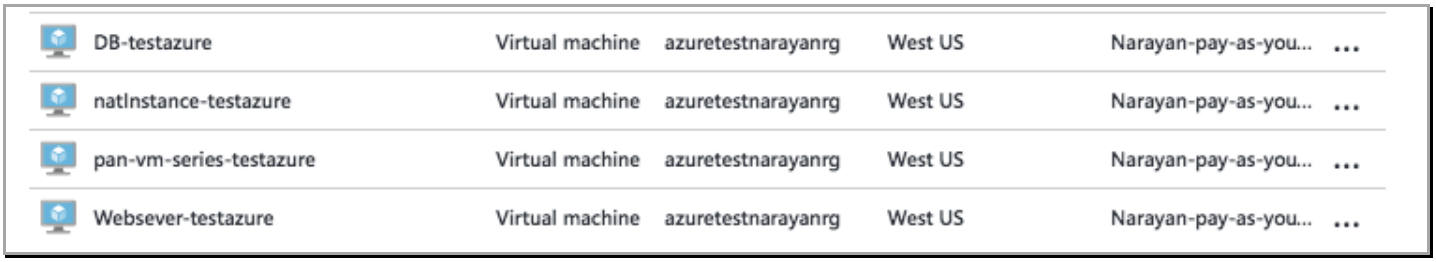
4. Review the Provisioned Resources

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



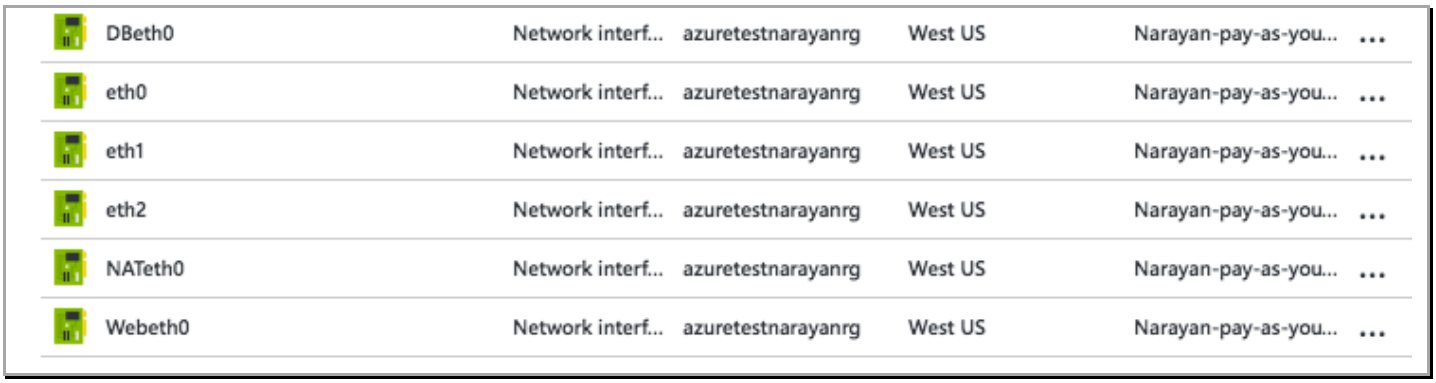
Here is a high level break down:

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



Network interfaces

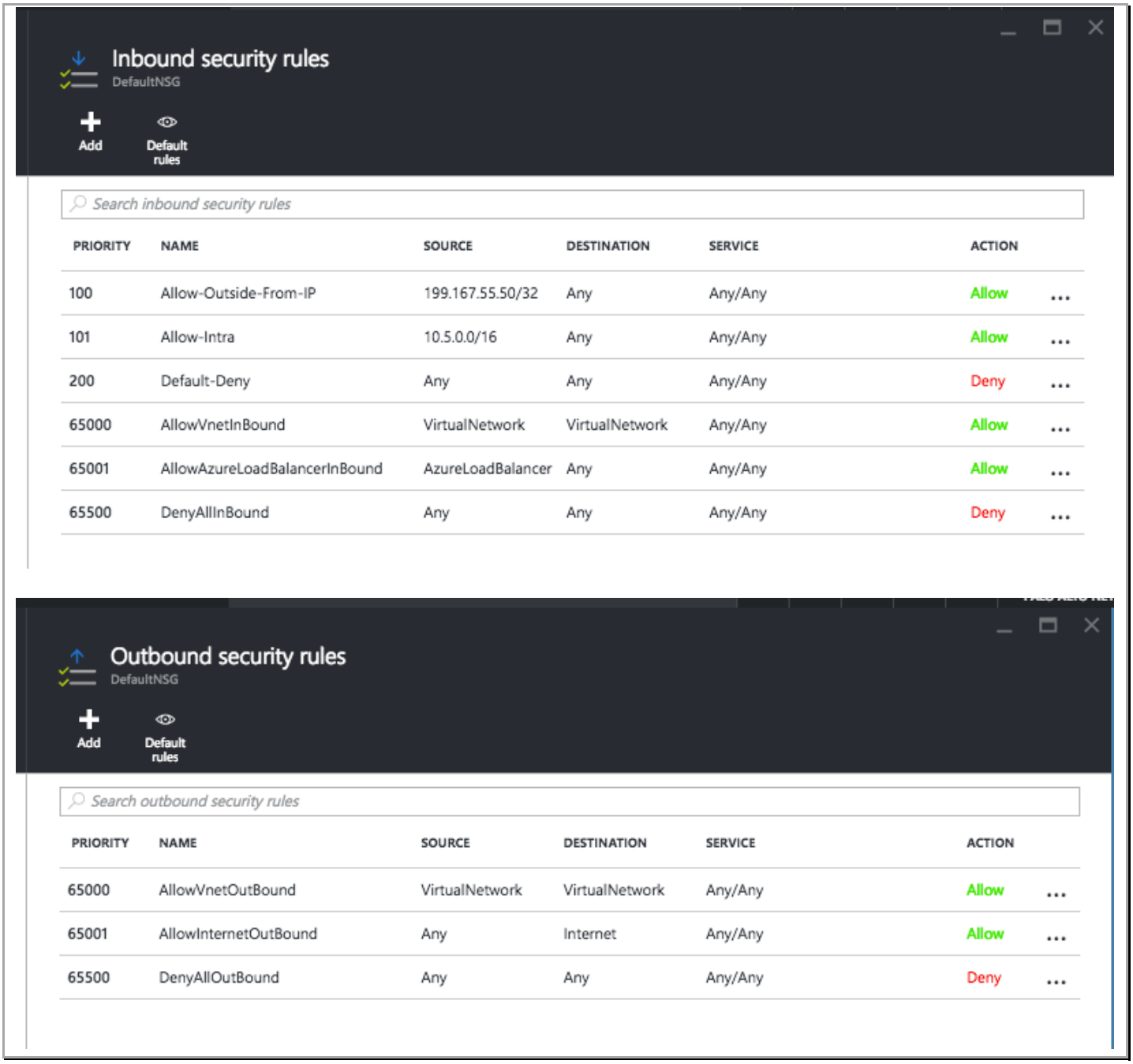
For the firewall: eth0 is the management interface, eth1 is in the untrust zone and eth2 is in the trust zone.



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.

Inbound and outbound rules for the DefualtNSG



Inbound security rules
DefaultNSG

Add | Default rules

Search inbound security rules

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

Add | Default rules

Search outbound security rules

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

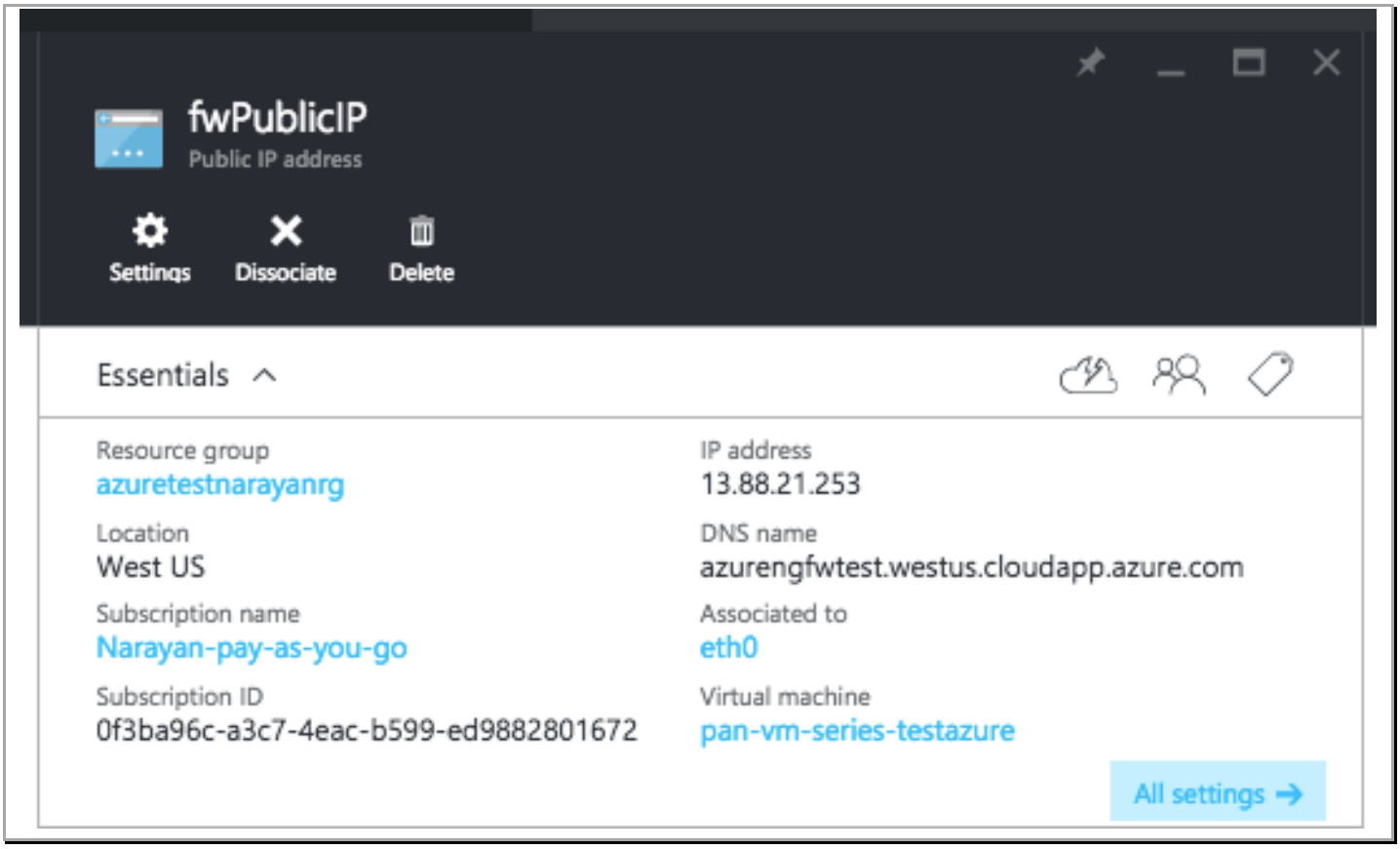
The above UDRs enable the VM-Series firewall to secure the Azure resource group. For the five subnets—Trust, Untrust, Web, DB, and NAT—included in the template, you have five route tables, one for each subnet with user defined rules for routing traffic to the VM-Series firewall and the NAT virtual machine.

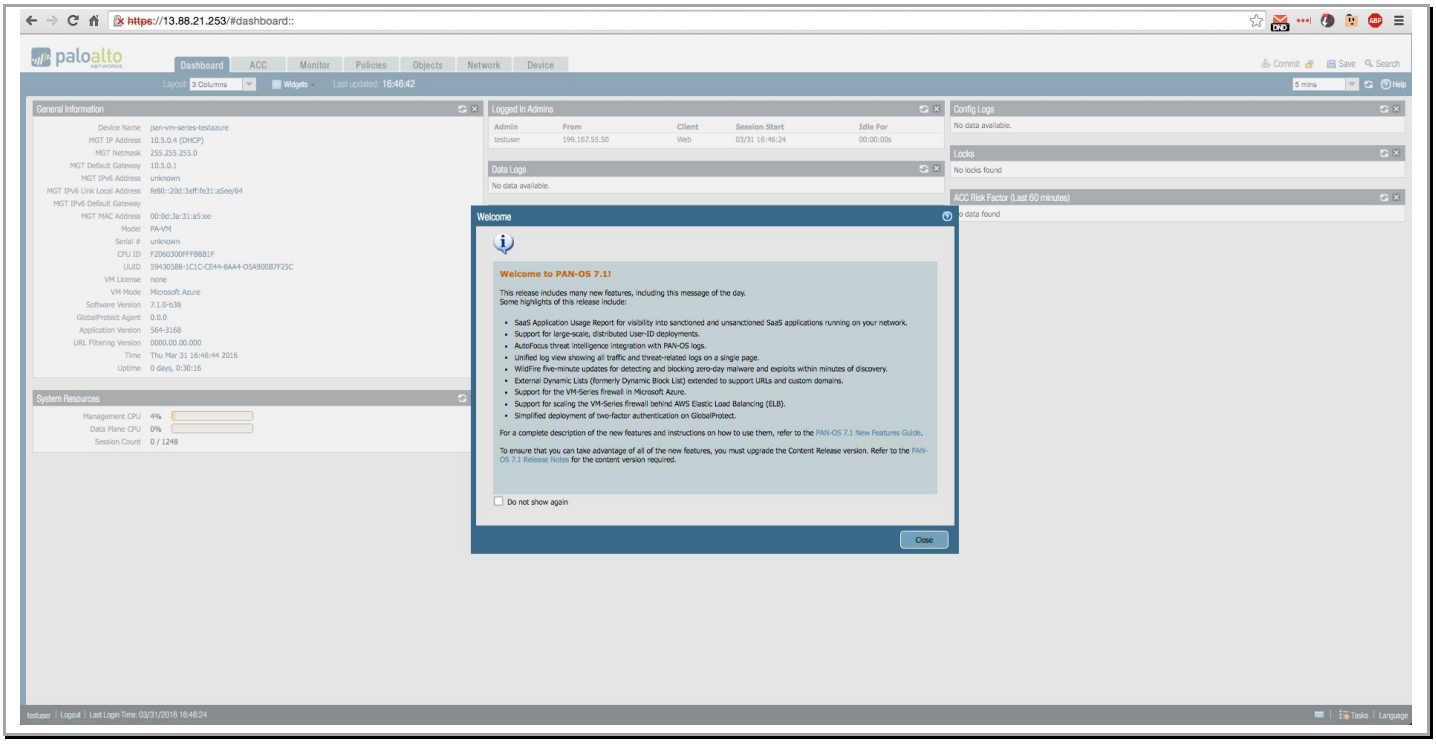
Public IPs

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





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.