VM-Series for Azure

Azure Resource Manager Template Deployment Guide

How to deploy a two-tiered application environment secured by the VM-Series firewall

http://www.paloaltonetworks.com

March, 2017

Table of Contents

Version History

Version number	Comments
1.0	Initial GitHub check-in
1.1	Removed NAT instance
2.0	Expanded guide to include activities

Support Policy

This ARM template 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.

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:

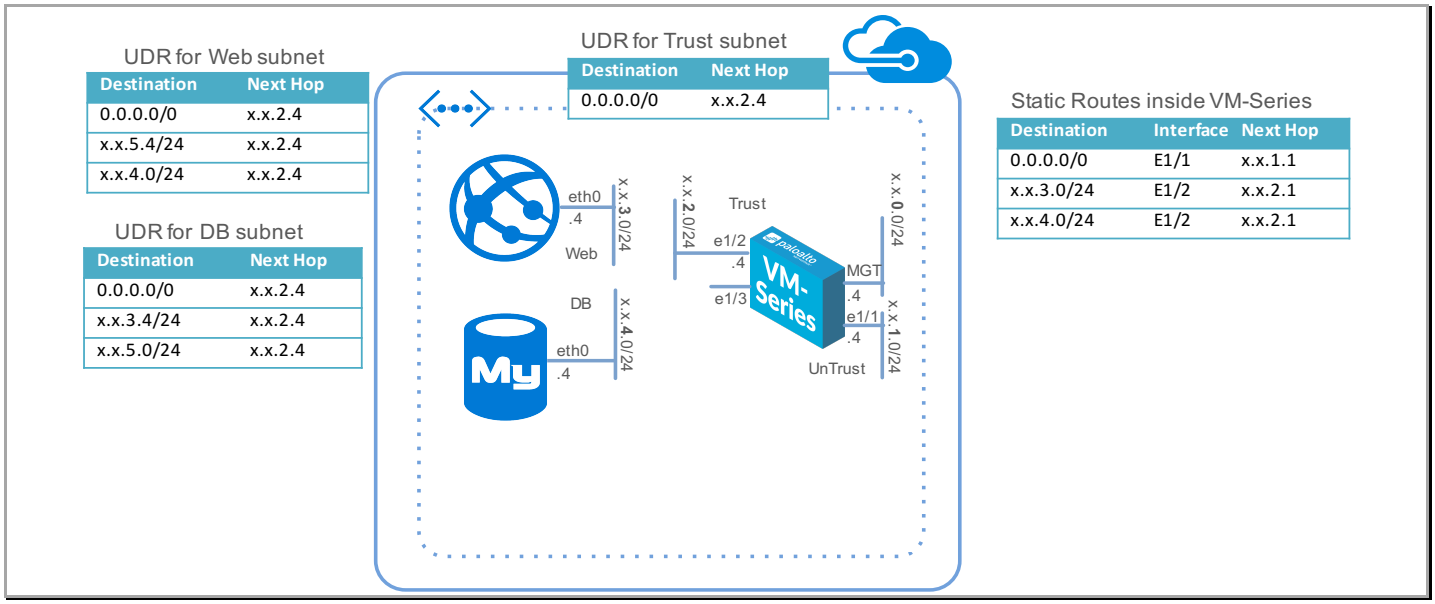
https://azure.microsoft.com/en-us/documentation/templates/

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, and two Linux virtual machines that are configured as a WordPress server and MySQL server respectively (representing a two-tier application environment). 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:



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

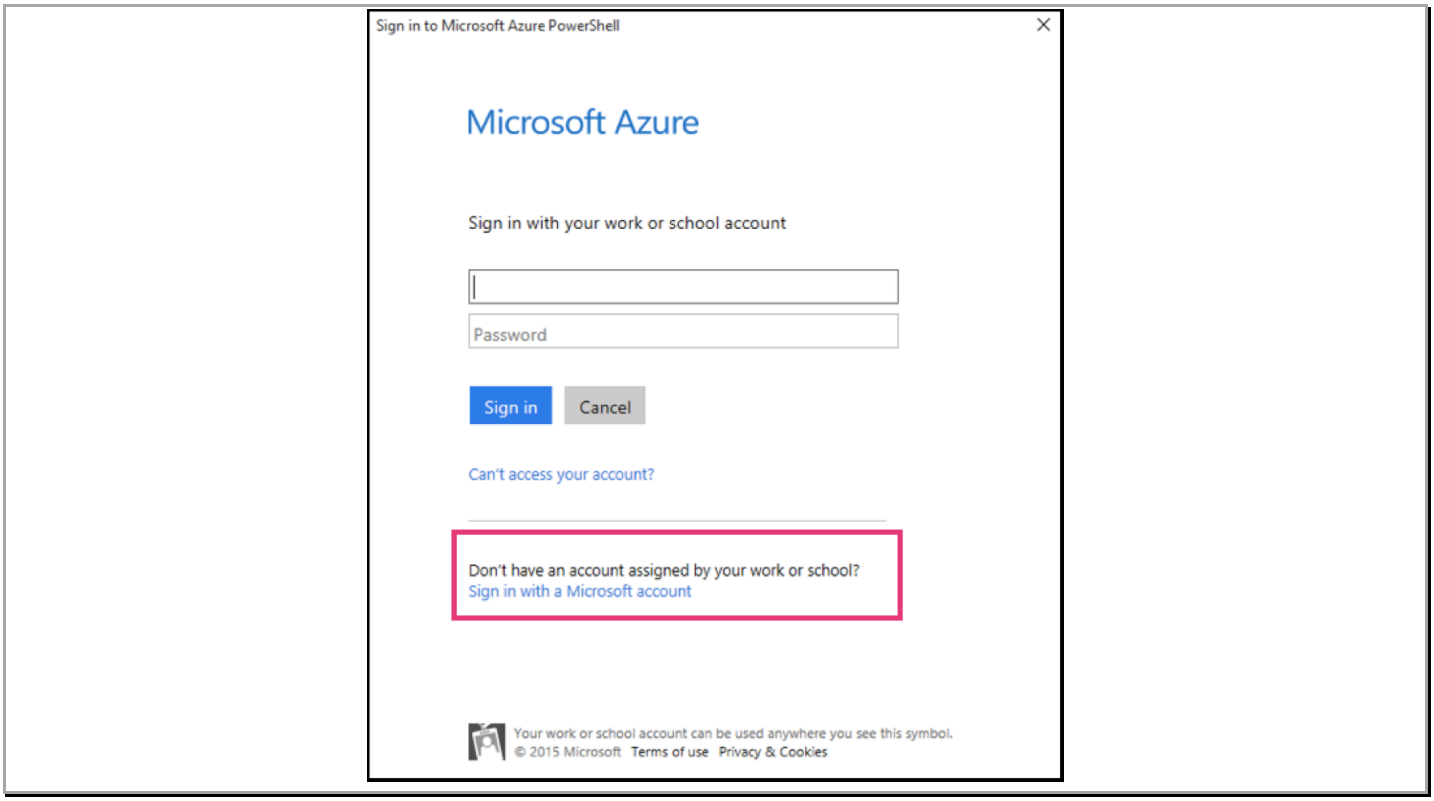
2. Prerequisites

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".



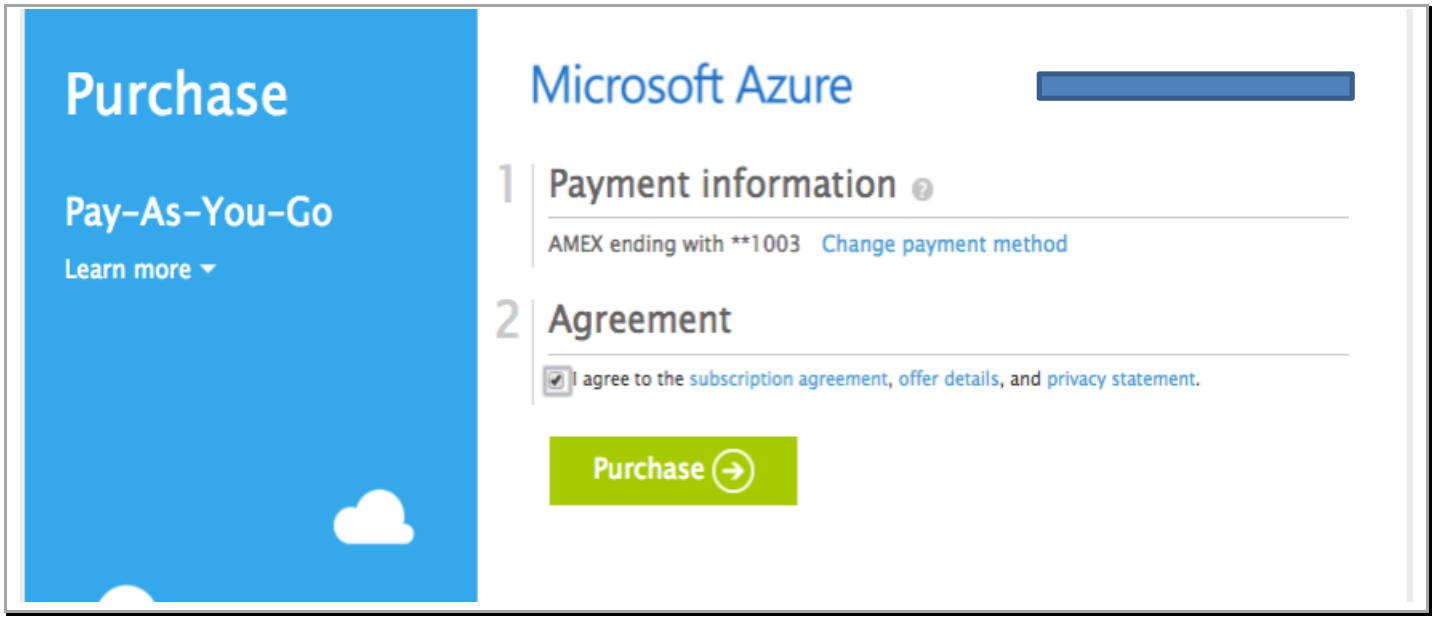
The free trial expires 30 days from account creation date or when $200 free credits are used up.

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**"

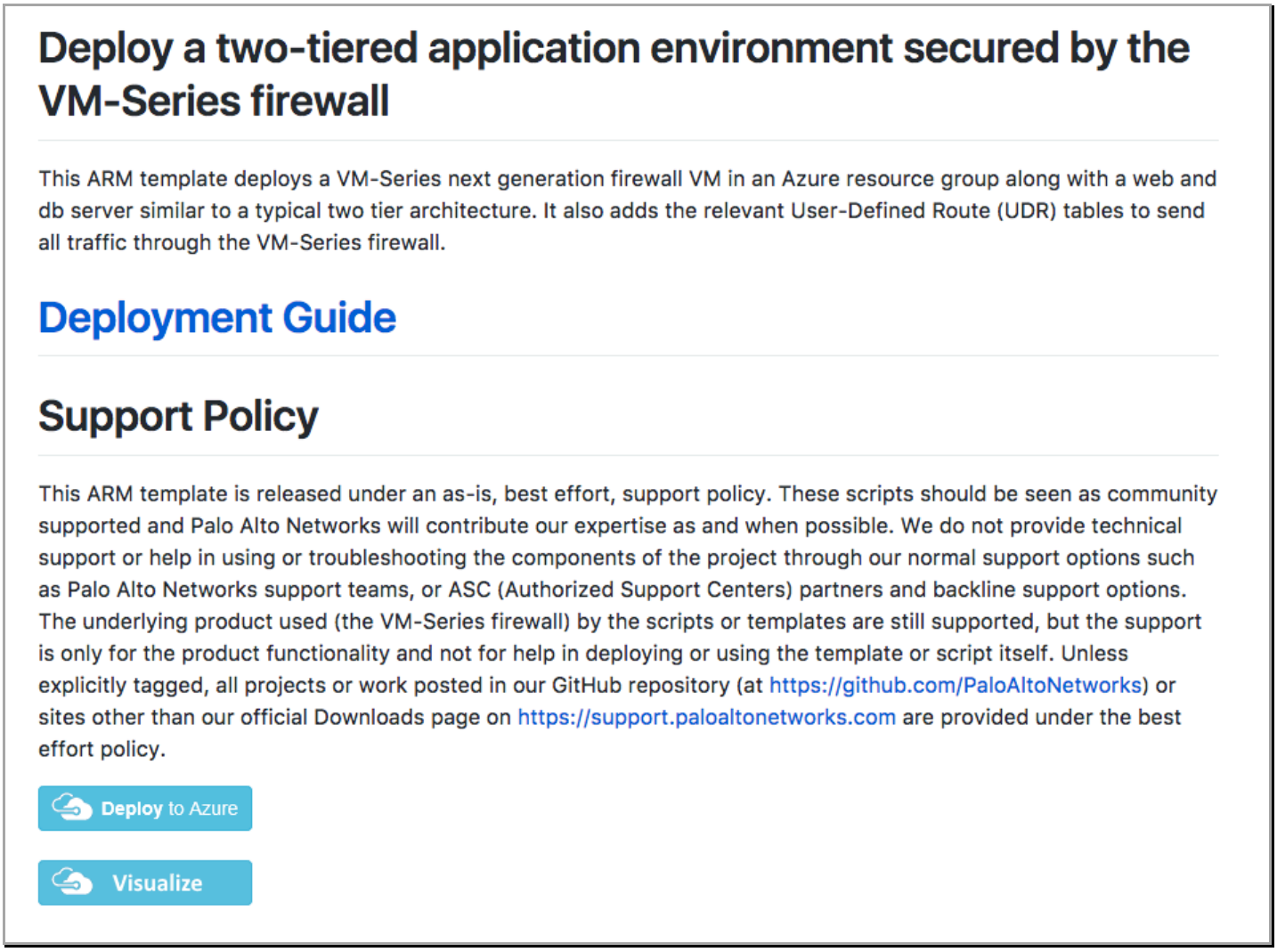


3. Launch the ARM Template

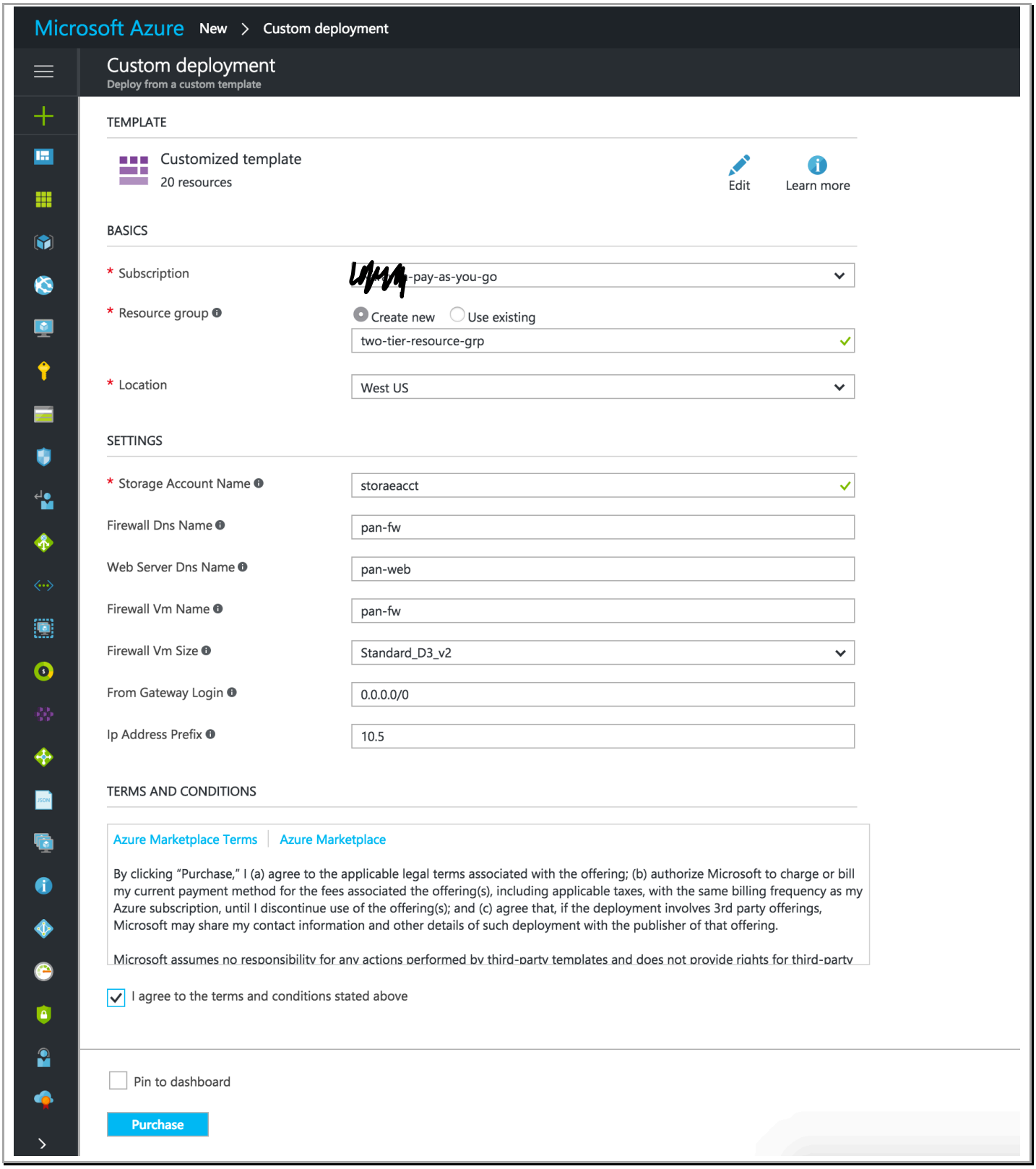
3.1 Deploy from Github

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/two-tier-sample 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.

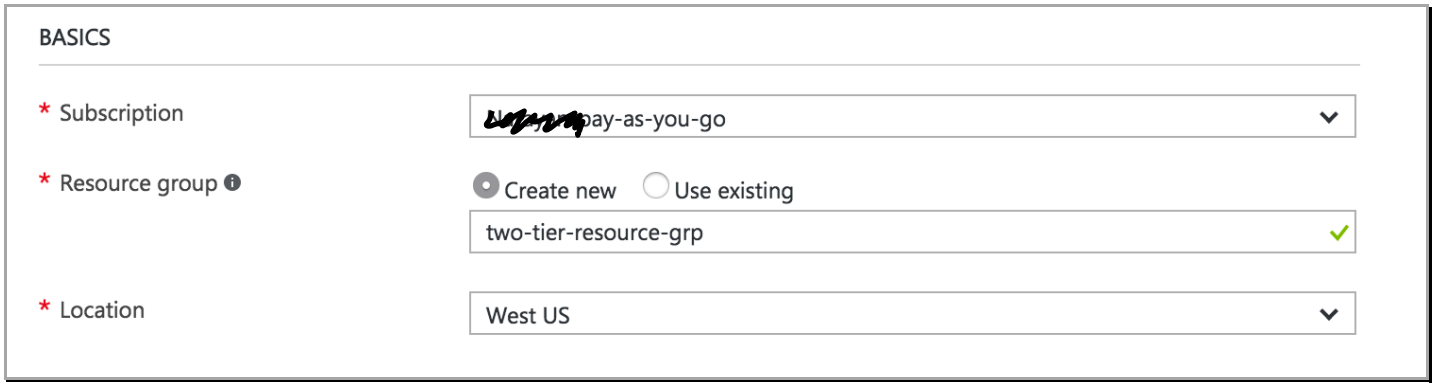

Microsoft Azure
New > Custom deployment
Custom deployment
Deploy from a custom template
TEMPLATE
Customized template
20 resources
Edit
Learn more
BASICS
* Subscription
-pay-as-you-go
* Resource group
Create new
Use existing
two-tier-resource-grp
* Location
West US
SETTINGS
* Storage Account Name
storaeacct
Firewall Dns Name
pan-fw
Web Server Dns Name
pan-web
Firewall Vm Name
pan-fw
Firewall Vm Size
Standard_D3_v2
From Gateway Login
0.0.0.0/0
Ip Address Prefix
10.5
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
Pin to dashboard
Purchase

3.2 The Parameters

You must specify the following parameters for your deployment.

1. Basics

Select your subscription, pick a unique resource group name and select a location where the template will deploy resources

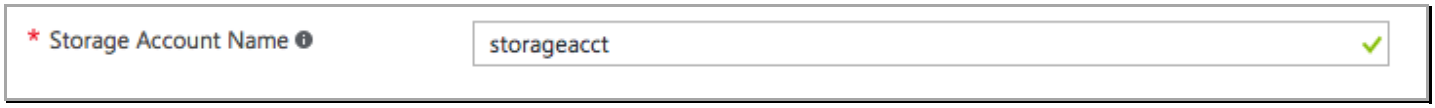


You can select an existing resource group into which the resources within the template will be deployed into. But, you will be responsible for cleanup of individual resources if you need to preserve the resource group.

2. Settings

Storage Account Name:

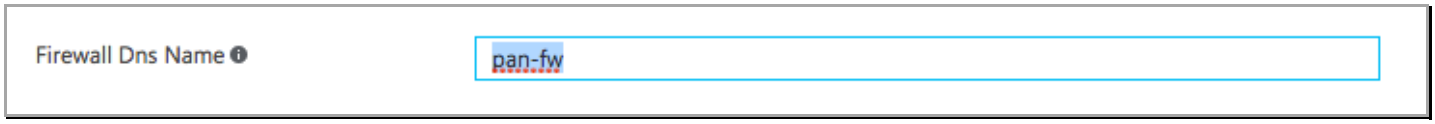
Specify the storage account name to use. This name has to be unique (so use your name or something else as a unique identifier). Also, only lower case letters and number are allowed. The name cannot have spaces, dashes or special characters. You can enter up to 20 characters



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

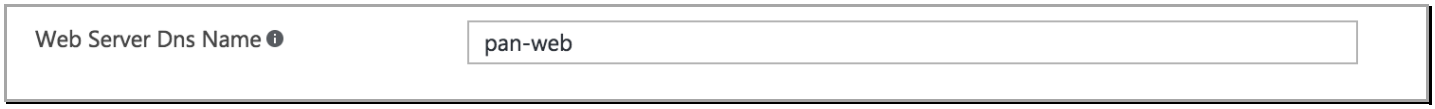
Firewall DNS Name:

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.



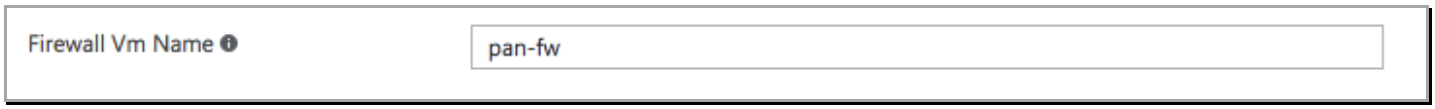
Web Server DNS Name:

This is the DNS name for the web server. Part of this name will be incorporated into the web server's URL



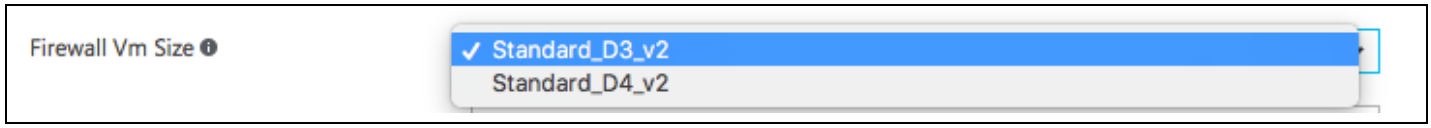
Firewall VM Name:

The name for the VM-Series firewall in the Azure portal



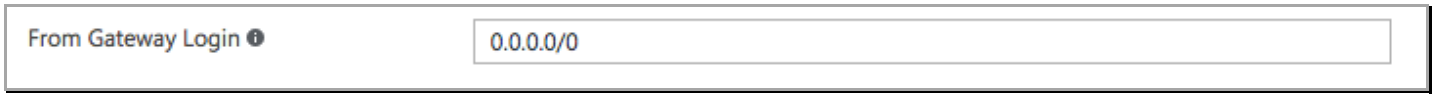
Firewall VM Size:

Select One of the two VM sizes for the firewall. For specifics of the instance sizes please refer to the following https://azure.microsoft.com/en-us/pricing/details/virtual-machines/linux/



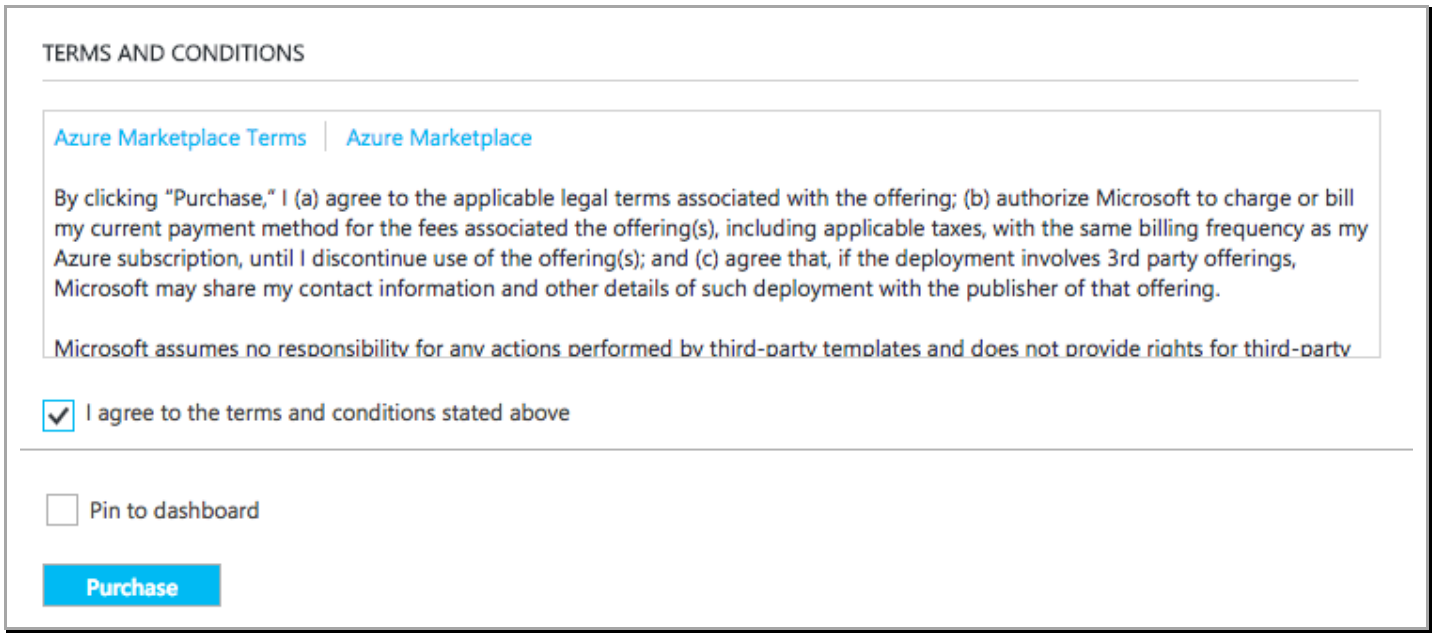
From Gateway Login:

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.



3.3 Agree to terms and Launch

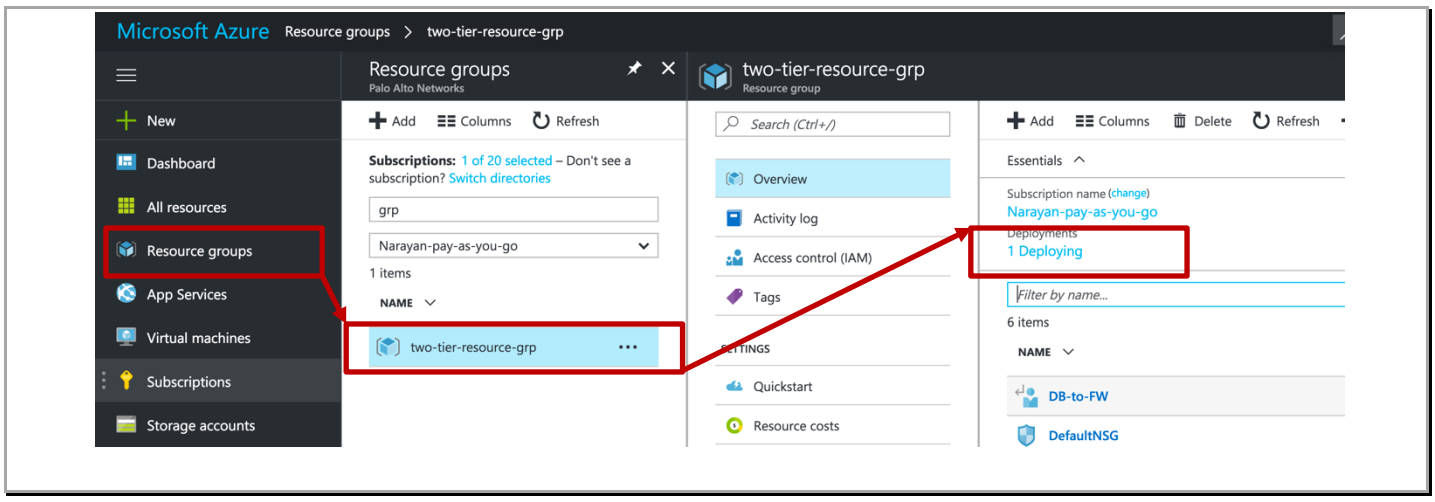
Agree to the terms and click **"Purchase"**

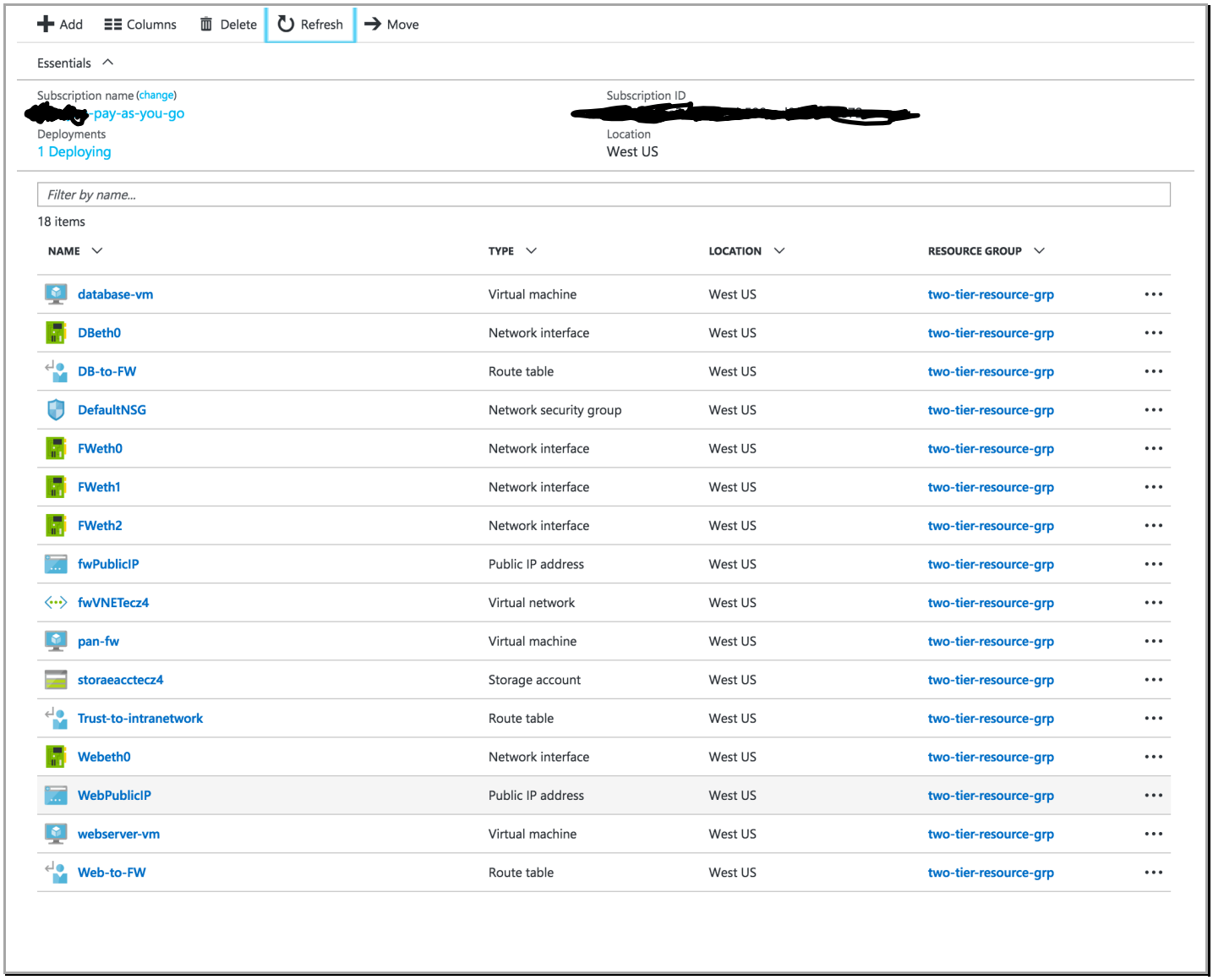


This will deploy the template and create resources.

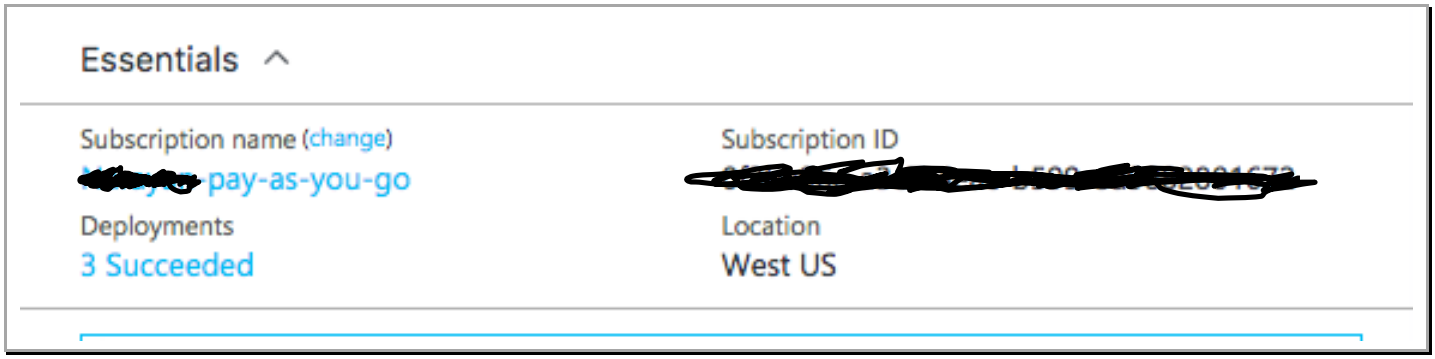
3.4 Check Deployment Status

If successfully deployed, select **Resource groups** on the portal to view the resource group that was created by the template, and under "**Deployments**" click the "**Deploying**" link to view all the resources that are being created.



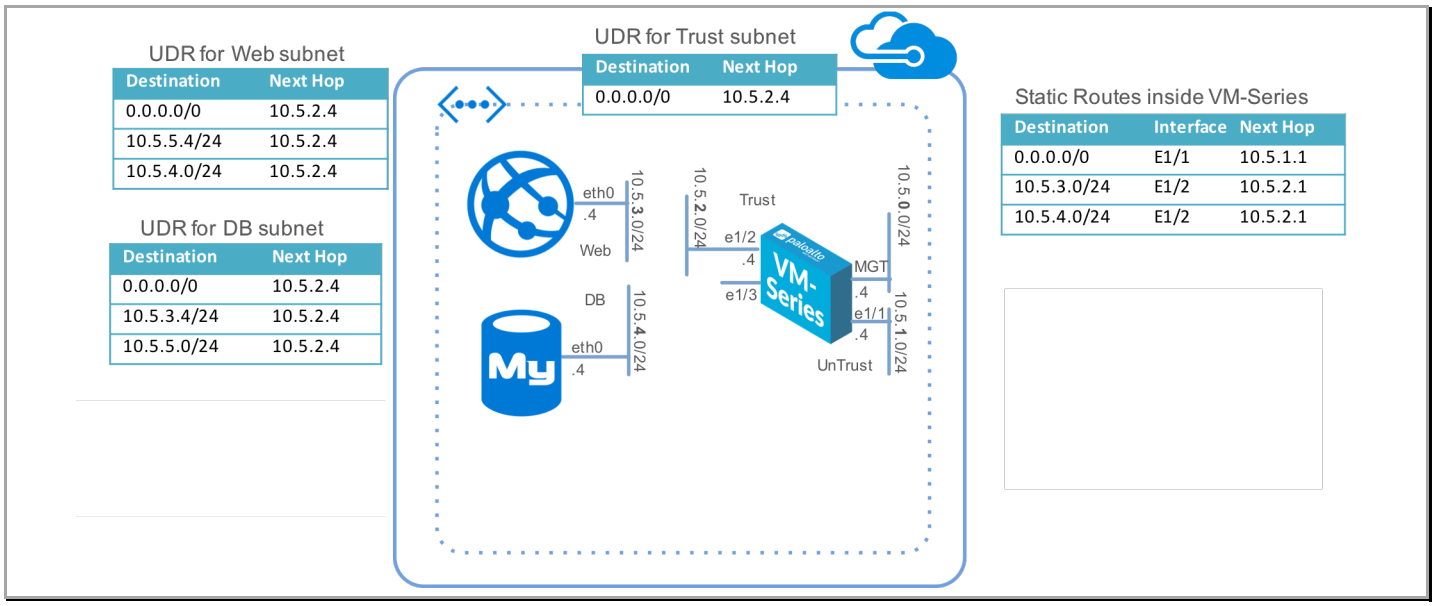


If the ARM template deployment was successful, the deployment state will show as "**3 Succeeded**"



3. Review the Provisioned Resources

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



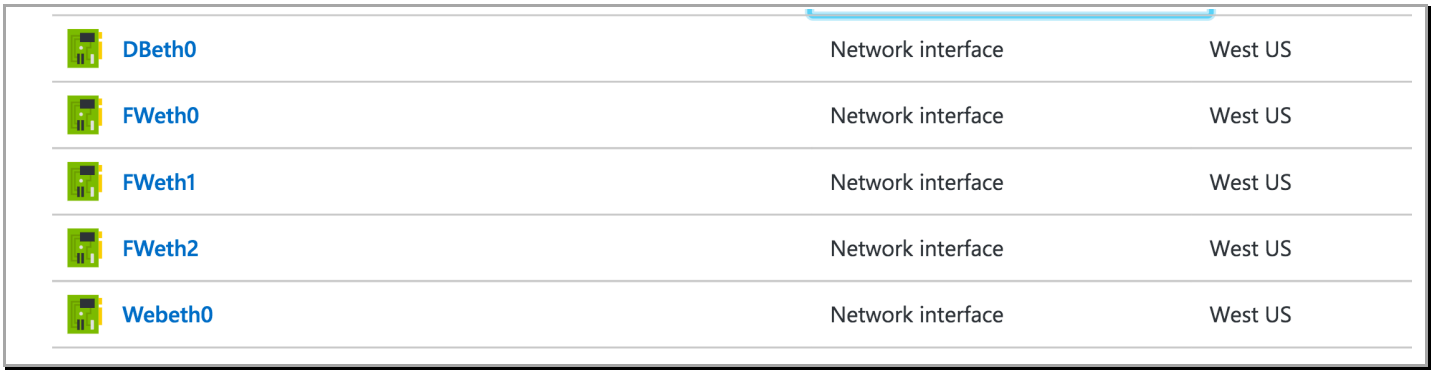
Here is a high level break down:

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

database-vm	Virtual machine	West US
pan-fw	Virtual machine	West US
webserver-vm	Virtual machine	West US

Network interfaces

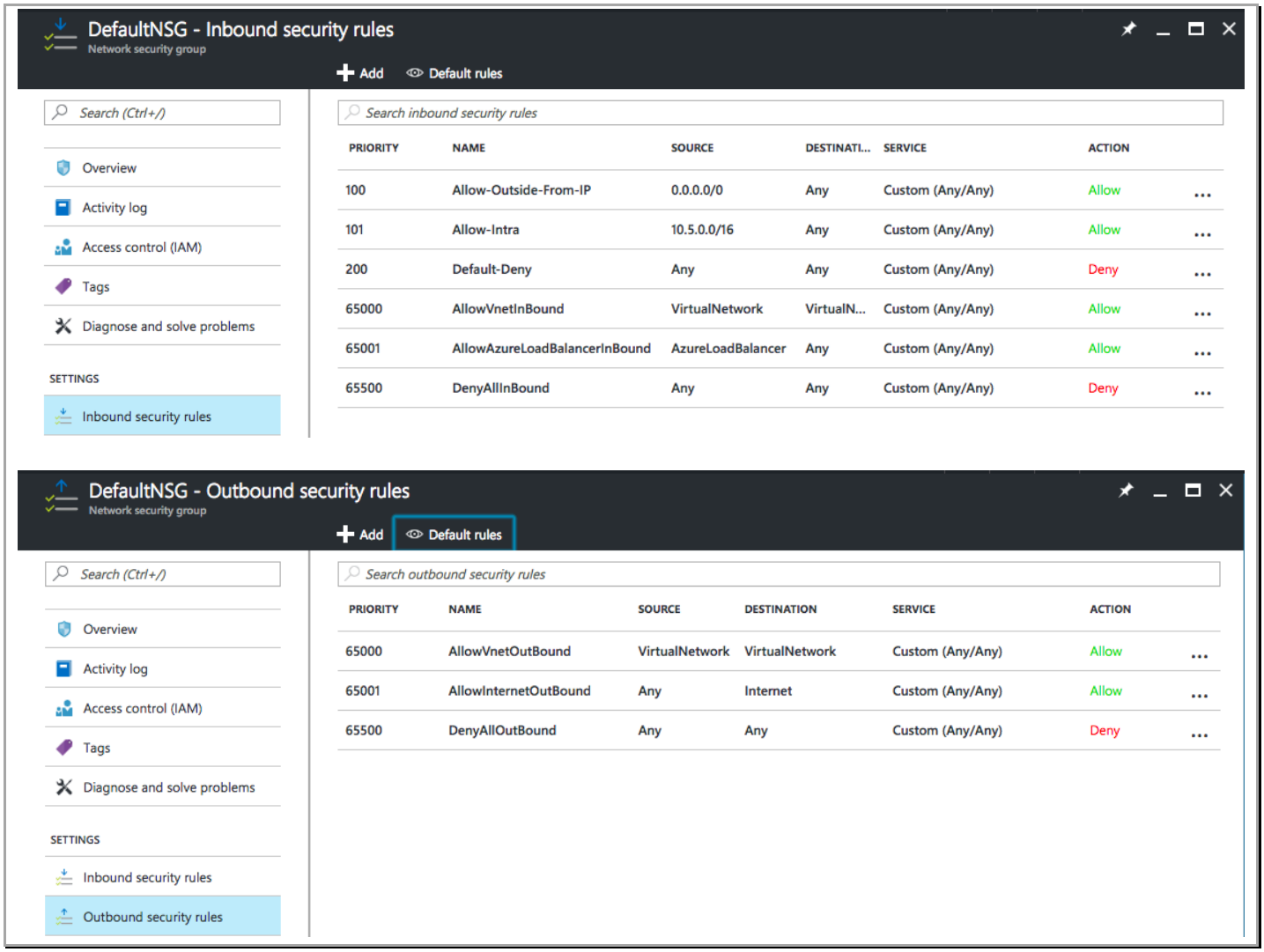
For the firewall: FWeth0 is the management interface, FWeth1 is in the untrust zone and FWeth2 is in the trust zone.



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

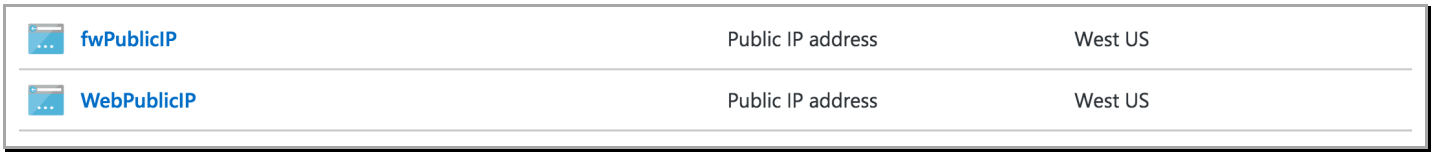


User defined Routes (UDRs)

DB-to-FW	Route table	West US
Trust-to-intranetwork	Route table	West US
Web-to-FW	Route table	West US

The above UDRs enable the VM-Series firewall to secure the Azure resource group. For the four subnets—Trust, Untrust, Web, and DB —included in the template, you have three route tables, one for routing traffic from the web to the FW, the DB to the FW and the Trust to the intra-network. Each UDR ensures that the traffic flows through the VM-Series firewall.

Public IPs



fwPublicIP	Public IP address	West US
WebPublicIP	Public IP address	West US

Custom Scripts/Linux Extensions

The template deploys Linux extensions to configure the firewall, web server (with Apache and WordPress) and database server (MySQL). Linux extensions are resources that can be used to configure Linux VMs. Each custom script downloads and runs a specific script (found in the Github repo) that configures a specific VM. The web-vm-customscript configures the firewall and the web server. The db-vm-custom script configures the database server

> Note: The entire template should take about 10 minutes to deploy and be fully functional

The next sections will guide you through the PAN-OS WebUI and show you how to safely enable applications

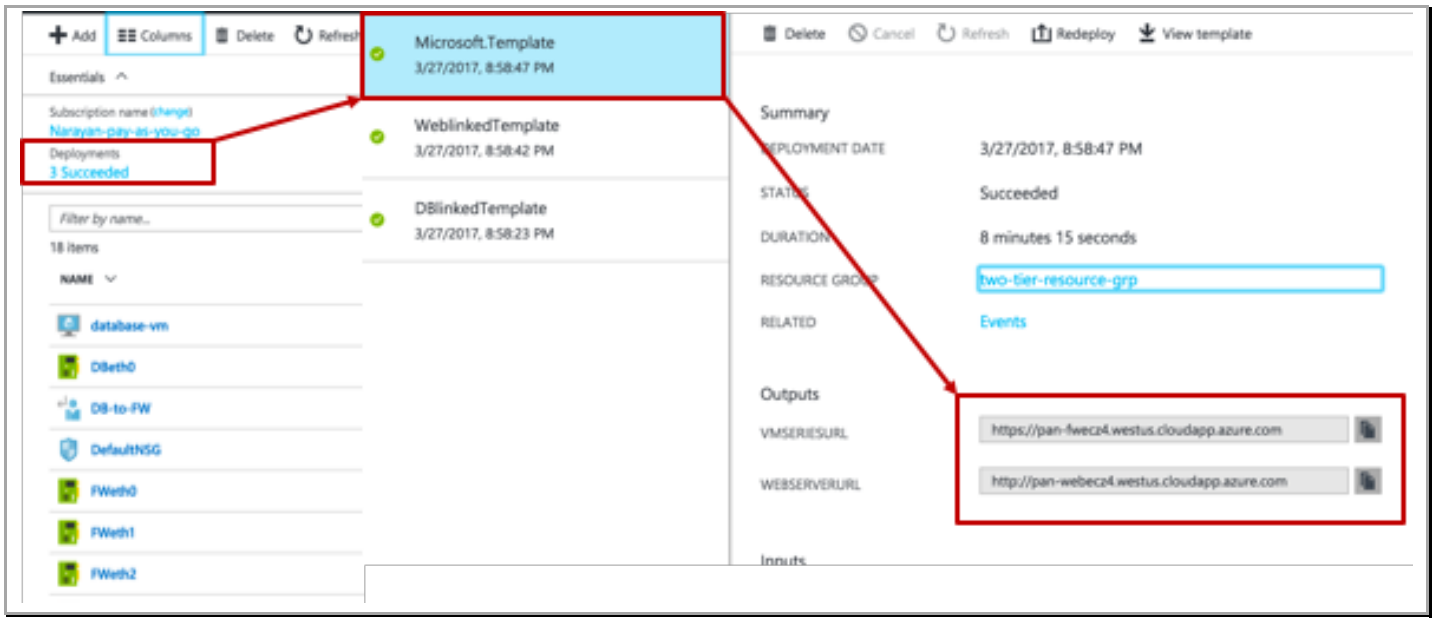
4. Activity 1 – Review PAN-OS WebUI

In this activity, you will:

- Login to the VM-Series firewall
- Review key portions of the firewall configurations

Task 1 – Login and Dashboard summary

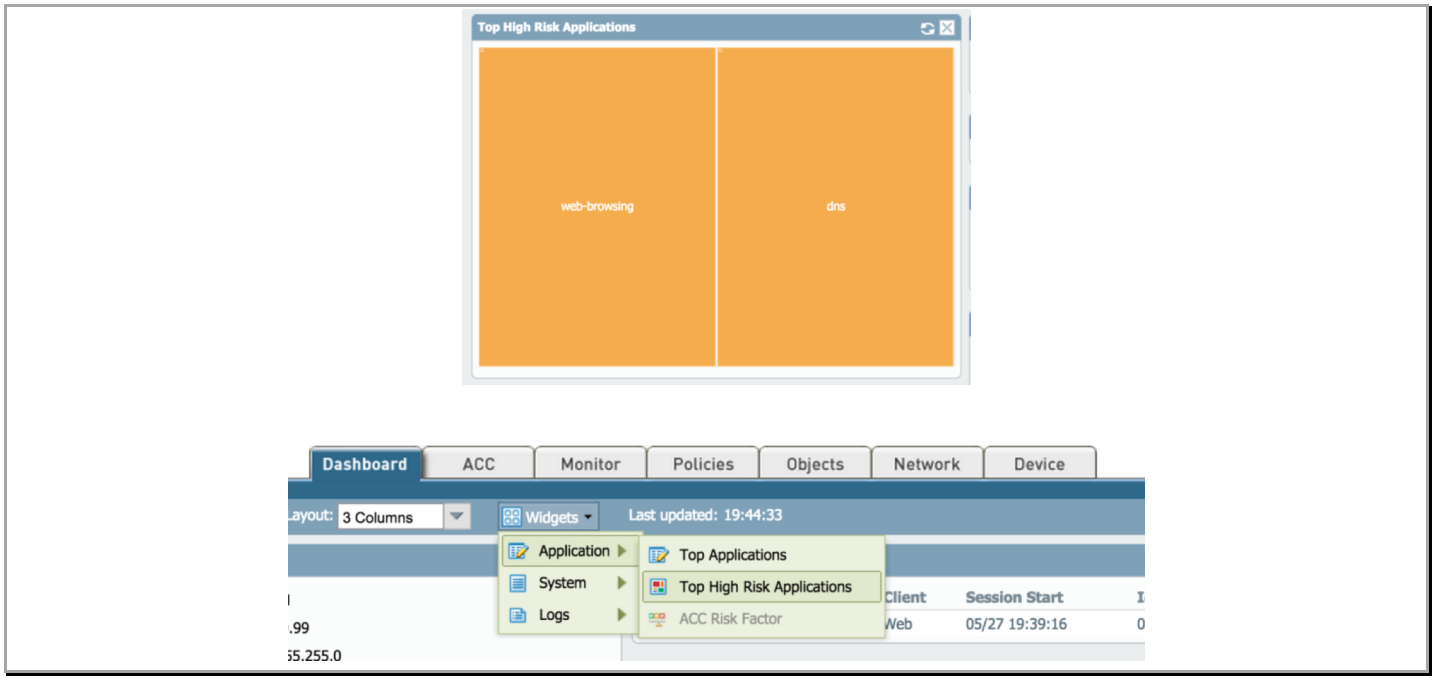
To access the firewall login page, access the URL from the azure portal template deployment summary page. You should be able to log into the **VMSeriesURL** using the username/password: paloalto/Pal0Alt0@123



> **Note:** Your browser will give you a certificate warning, you can safely acknowledge it and proceed.

Upon login, you will see the dashboard for the VM-Series. The dashboard provides a visual summary of the device status. It is widget-based and can be customized to fulfill your specific requirements. In the ***General Information*** widget, you can see this VM is a ***Microsoft Azure*** instance under the ***VM Mode***.

> **Note:** Since this firewall is brand new, it likely doesn't have any traffic yet and your screen won't match the screenshot below. You can return to the dashboard at the end of the lab to see real data.

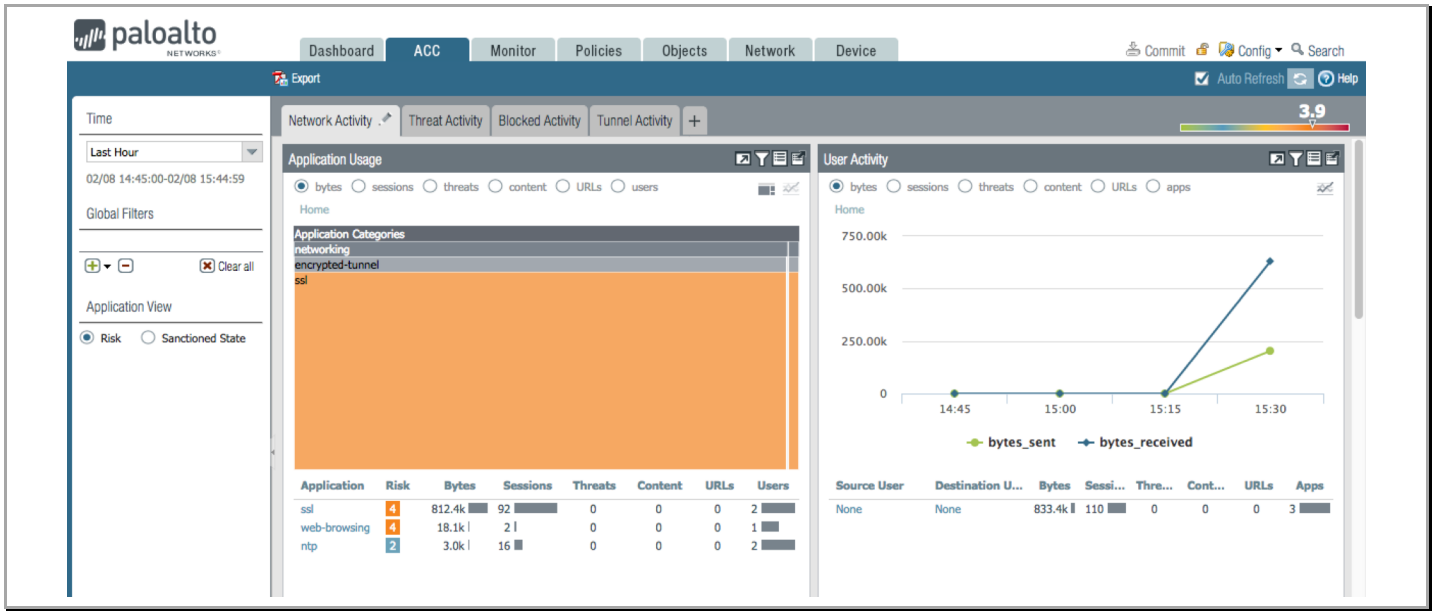


Task 2 – Application Command Center (ACC)

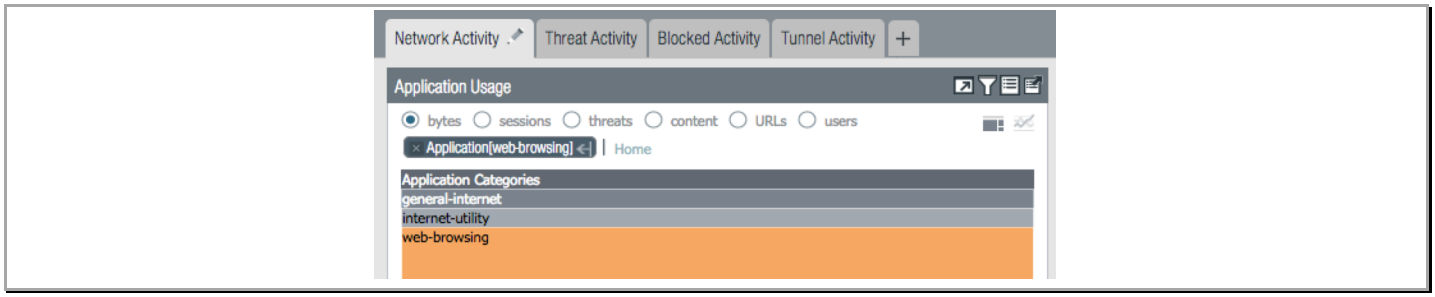
The ACC provides you with a widget-based summary of the applications, the content within, and who the user is over a given time period [default is 1 hour]. With the ACC, you can see the contextual linkage between the application and the content, which allows you to make more informed security decisions.

Select the ***ACC*** Tab:

The default ACC view will show you the network, threat, blocked and tunnel activity in four separate tabs for the past hour. As shown in the image below, the time frame and each tab can be customized to display the relevant application, threat, and user activity depending upon the user role. Additional tabs can be added via the + sign on the right side of the Blocked Activity tab.



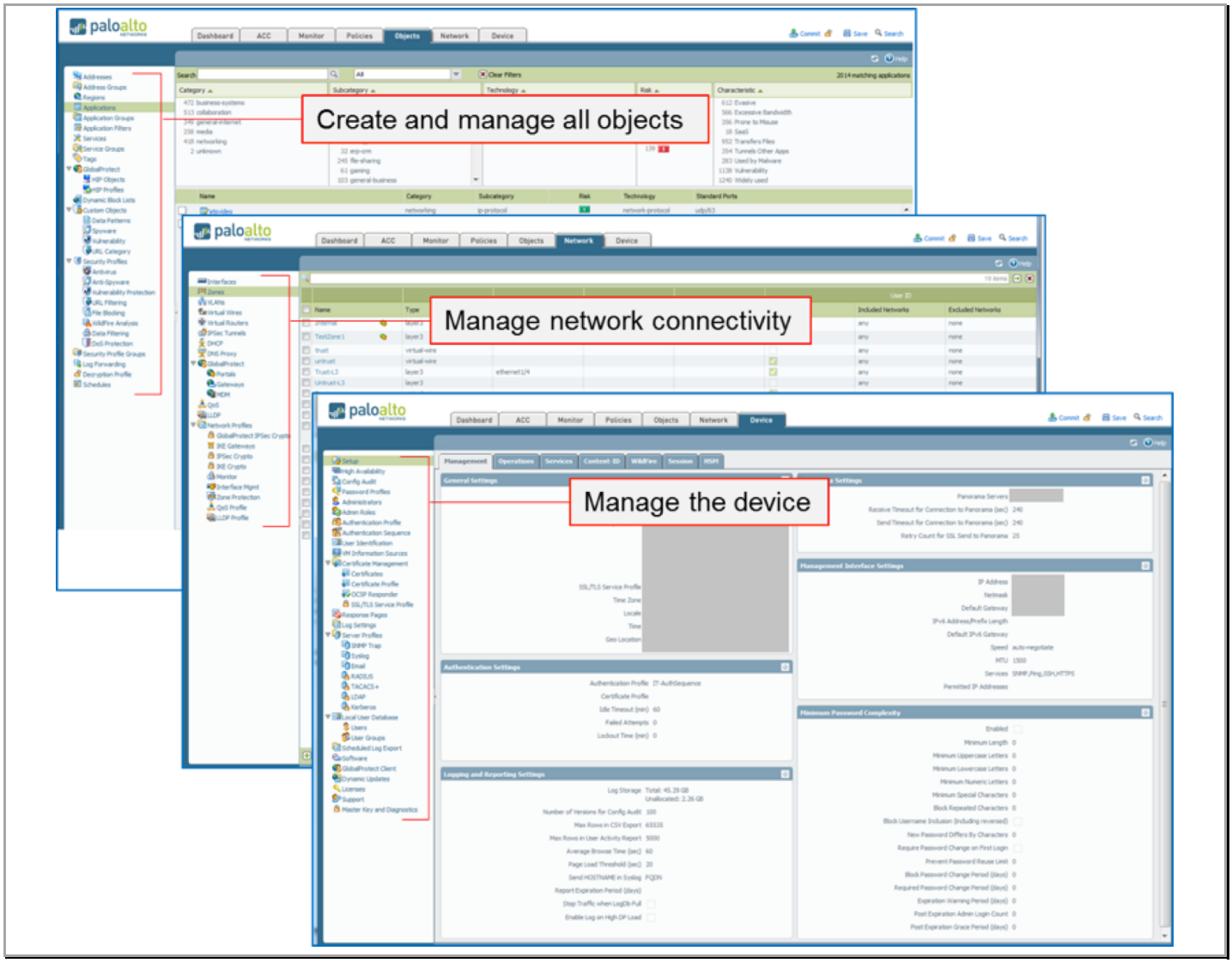
Within each of the widgets, you can select the relevant data point to learn more about what it is and what it means, and you can “Promote” that data point as a filter by clicking on the arrow to the right of the filter, which in turn will force all other widgets to be updated based on that context. Because you are viewing a brand-new firewall, there won’t be much data in this view yet.



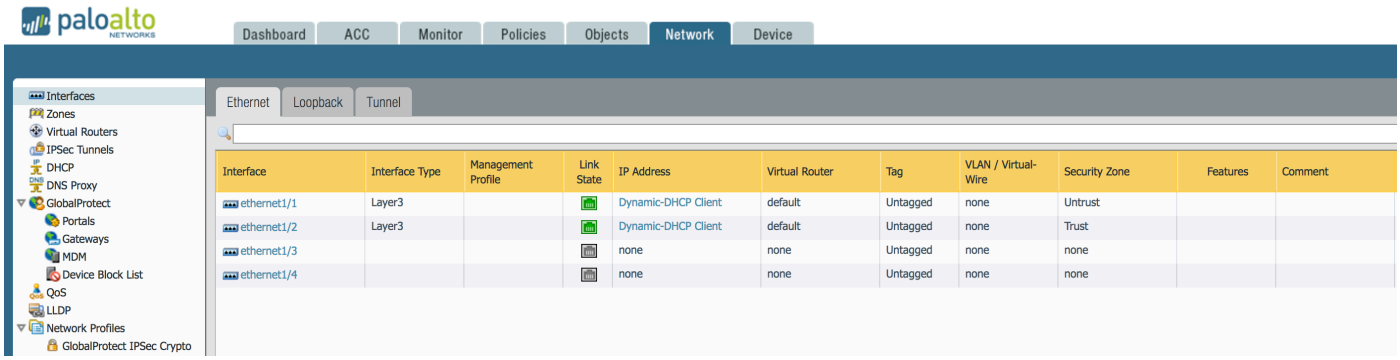
Task 3 – The Object, Network and Device Tabs

The Objects, and Device tabs provide you with the various management capabilities.

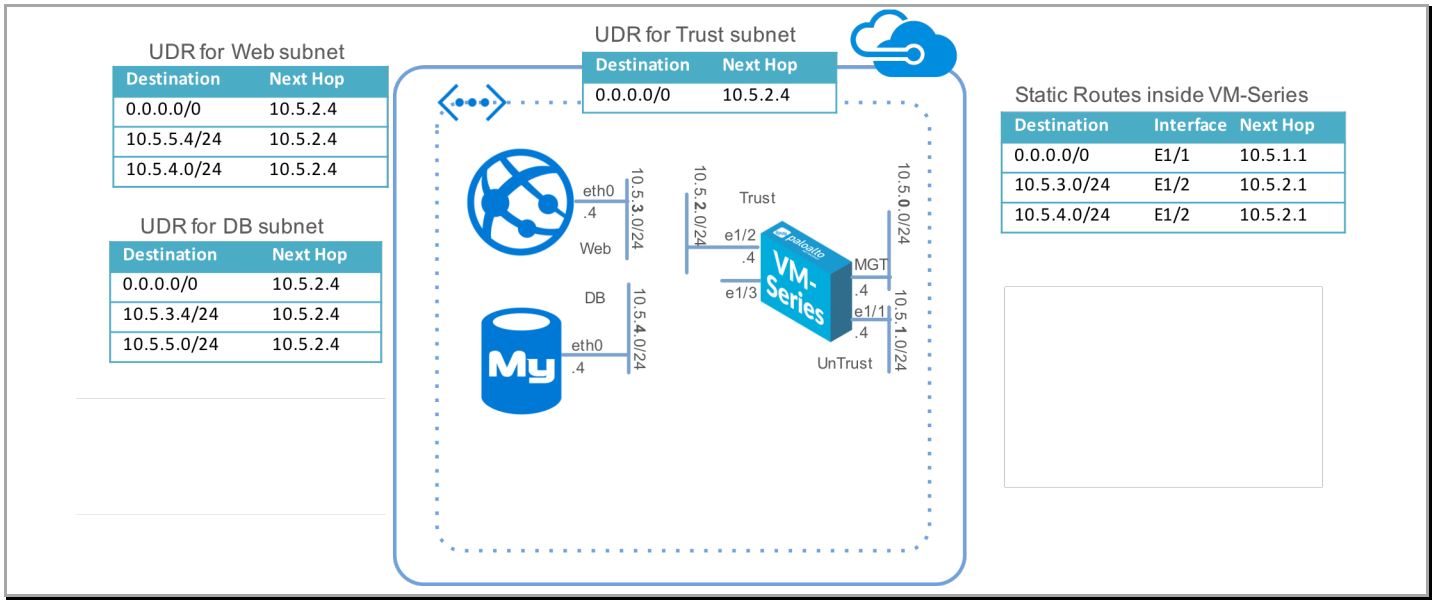
The Objects tab allows you to manage the building blocks for creating policies such as address objects, custom applications, and security profiles.



The network tab allows you to create and manage interfaces, security zones, VLANs and other elements that enable connectivity. Click the *Network* tab:



The network configuration should align with the following topology



The interface (Ethernet 1/1) in the *Unturst* zone is the interface that is exposed to the outside world. All traffic enters through this interface.

The interface in the *Trust* zone (Ethernet 2/2) is the interface where the assets that need to be protected reside (in this case the web and database servers).

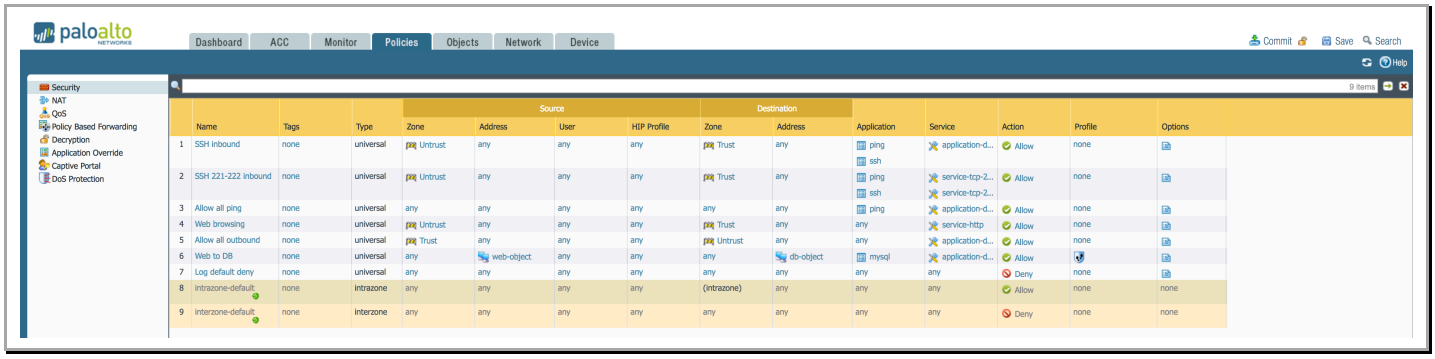
The Device tab is where configuration items like DNS, service routes, etc. are managed. The device tab also allows you to manage high availability, users, software and content updates.

Task 3 - Security Policies

The Policies tab is where you will define all of your policies. The default view will be your security policies, all of which can be based on the application, the content within, and the user. As shown

along the left side of the image, additional policies can be defined for actions such as NAT, Decryption, and DoS.

Select the *Policies* tab:

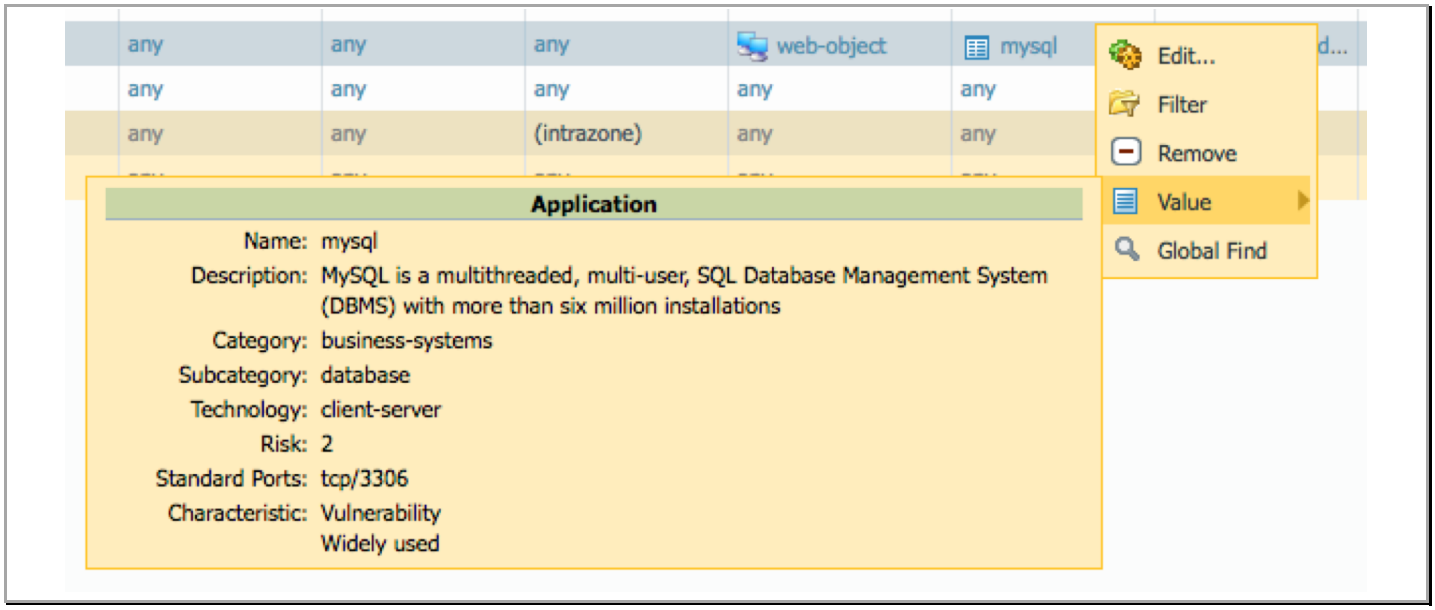


These policies are defined to allow ssh access on ports 221 and 222 to the web and db server respectively (for troubleshooting purposes), secures N/S traffic and E/W traffic between zones.

And the NAT policies allow for ssh access to the web and db servers as well as directing web traffic to the web server only.

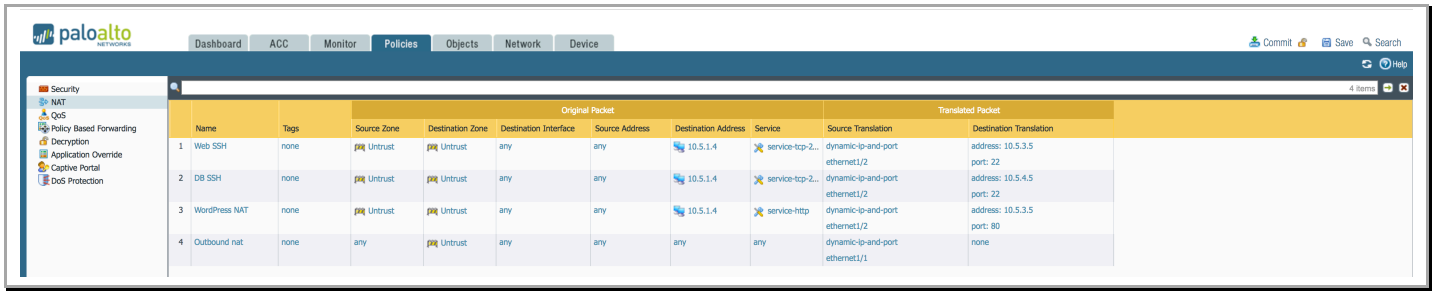
In the ***Web to DB*** rule (rule 6) and under the ***Application*** column, click on the small arrow next to ***mysql***.

Then click on ***value*** to see the details for the mysql AppID. You will see details about the application including the standard ports



Note: The VM-Series is a next generation firewall. It does not simply assume all traffic on TCP port 3306 is MySQL. It inspects the traffic and ensures that it truly is MySQL.

On the left-hand side, under *NAT* you can also inspect that translation rules that allow the web and db servers to be accessed from the outside world via SSH. A NAT rule that allows http access to the web server and a default outbound NAT rule to allow the web and db servers to access external resources.

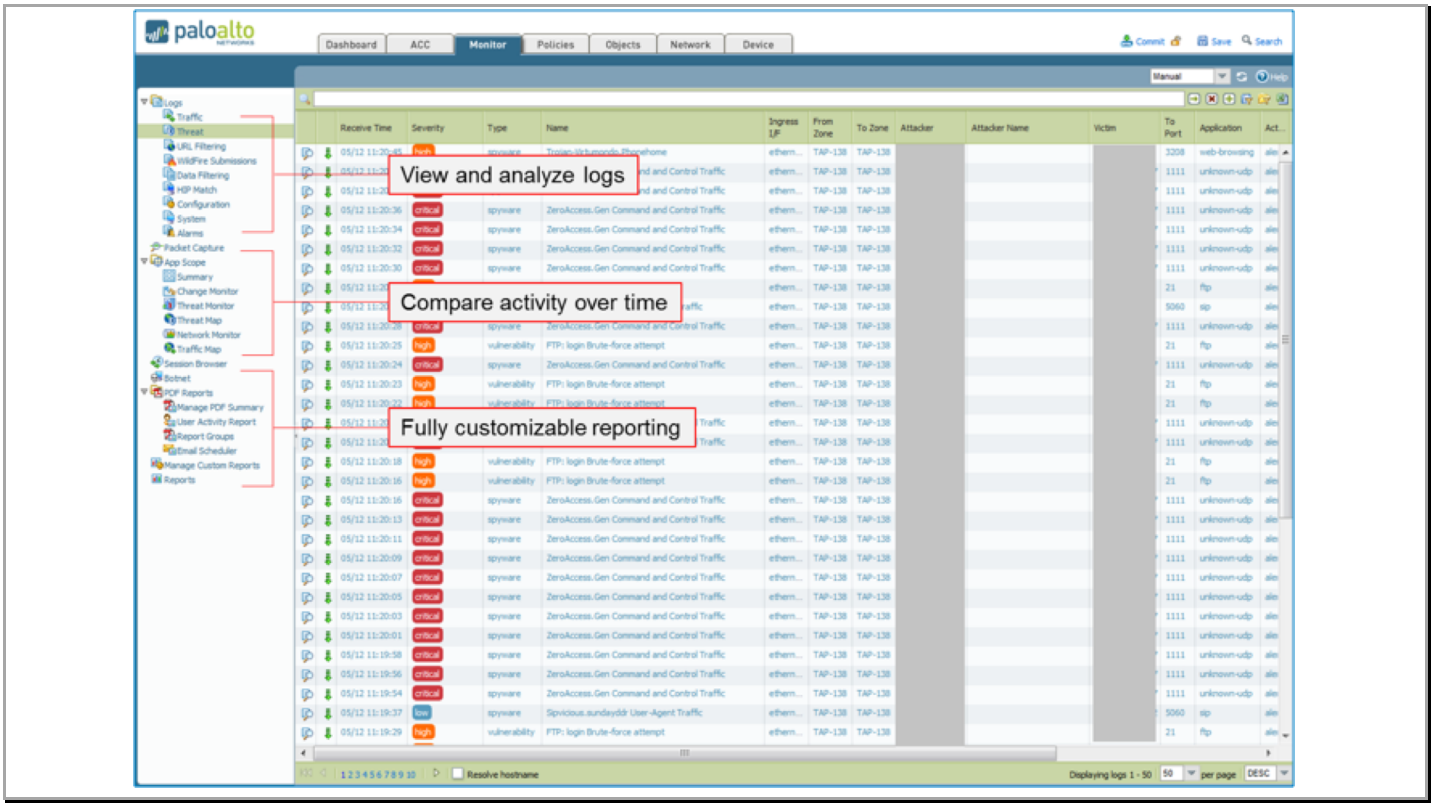


Task 4 – The Monitor tab

The Monitor tab is where you can perform log analysis and generate reports on all of the traffic flowing through the VM-Series. Logs are stored on box and can also be forwarded to either Panorama, our centralized management solution, or forwarded to a syslog server for analysis and reporting by 3rd party offerings

Navigate through the various log viewers, click Reports to see the various pre-defined reports you can use.

> **Note:** Your firewall is new and doesn't have any data yet so any reports you create at this point will likely be blank. You can return to this step at the end of the lab and create new reports.



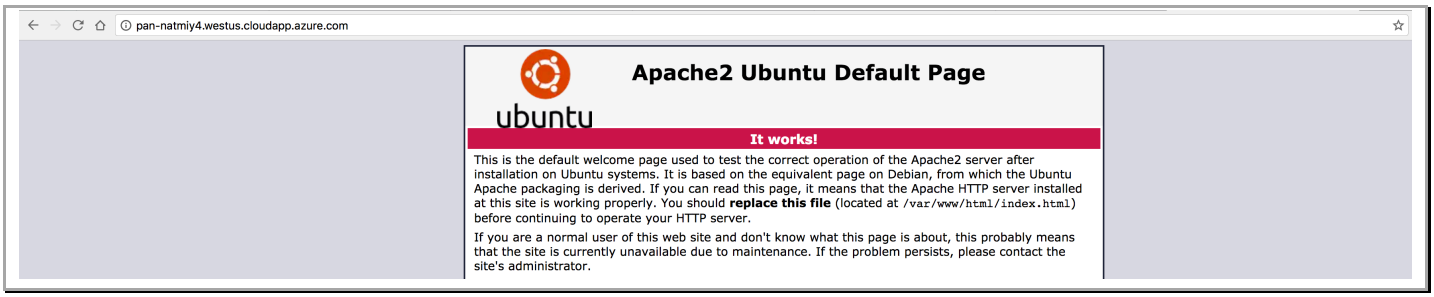
5. Activity 2 – Safely Enable Applications

In this activity, you will:

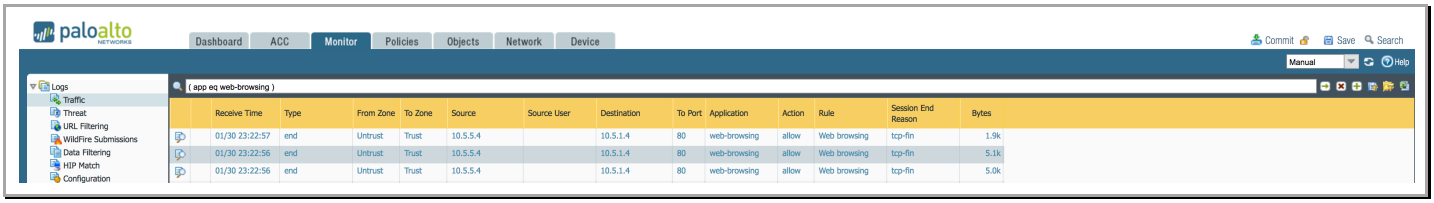
- Generate traffic on the firewall and review the traffic log
- Edit the security policy to allow inter-tier application traffic

Task 1 – Verify Static Content on Web Server

Using the second URL (WebserverURL) in the output section of the deployment summary access the static content of the webserver and you should see:



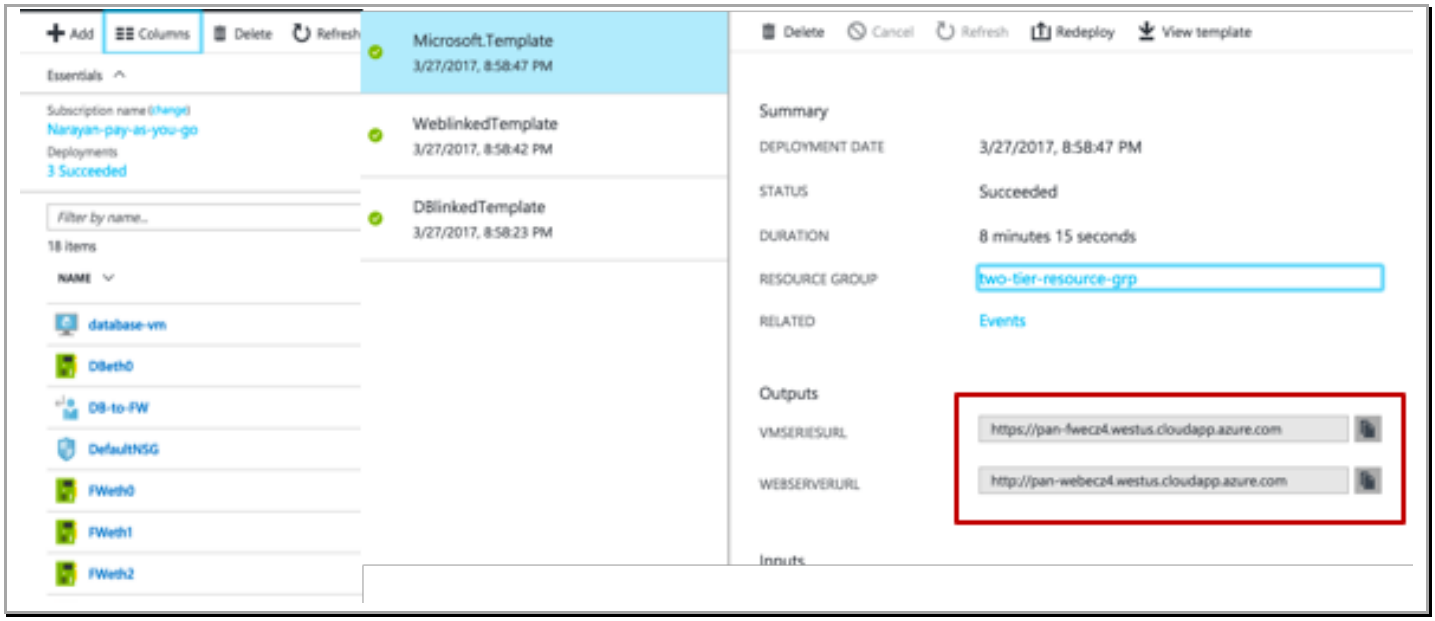
Check firewall logs to verify that the traffic is passing through the firewall:



Task 2 – Verify Dynamic Content on Web Server

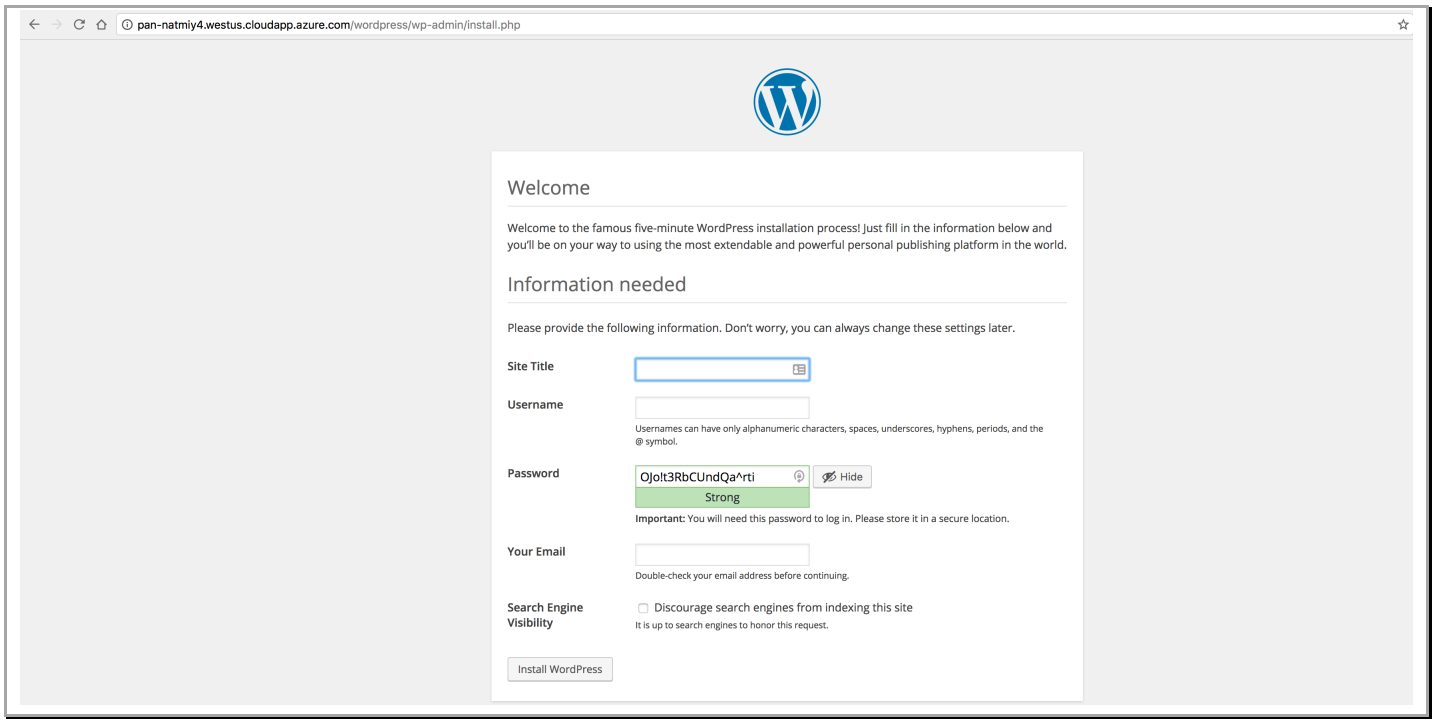
In this task, you will generate a WordPress content request from your web browser that will trigger a database query to the MySQL server. Like many web-based applications, WordPress uses a backend database to create, store, and retrieve dynamic content. You will use the WordPress application to show exactly this type of behavior and demonstrate how the VM-Series firewall will secure this traffic.

In the browser, head to the WordPress server (http://webserverURL/wordpress) this should be the second link in the output section of the deployment tab

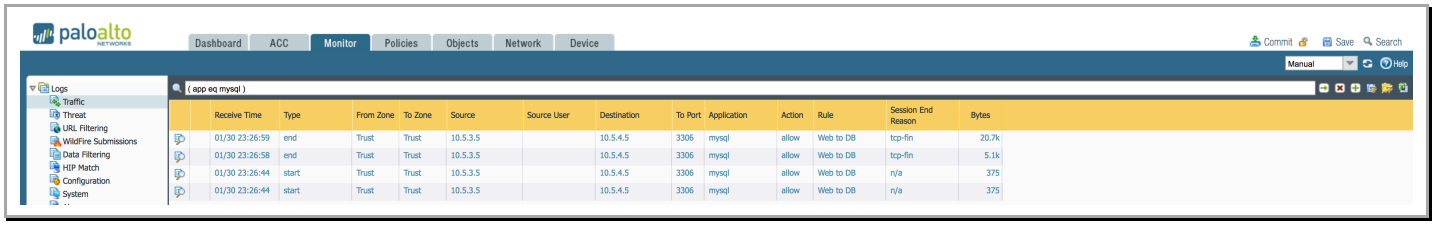


And you should see the WordPress welcome page.

Note: You don't need to actually configure the new WordPress server. In its initial, un-configured state, it will generate the traffic we need to test the VM-Series firewall.



Now, head back to the firewall and verify that the traffic did indeed go through the firewall from web to db:



6. Activity 3 – Safe Application Enablement

In this activity, you will:

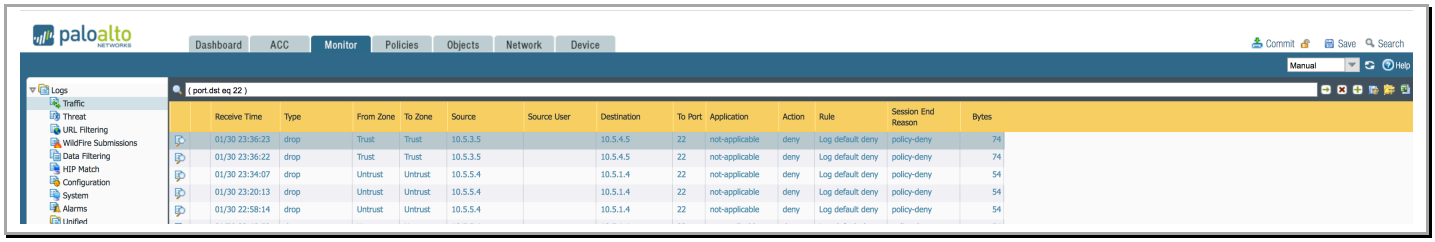
- Generate two simulated east/west (web tier to database tier) attacks
- Monitor the firewall logs to see the results of the attacks

Task 1 – Attempt to SSH from the web server to the DB server

This task will simulate a compromised web server that is being used to attack the database. This is a common attack strategy of getting a foothold on the web front-end server and then expanding to the other application tiers with the ultimate goal of accessing all data in the database.

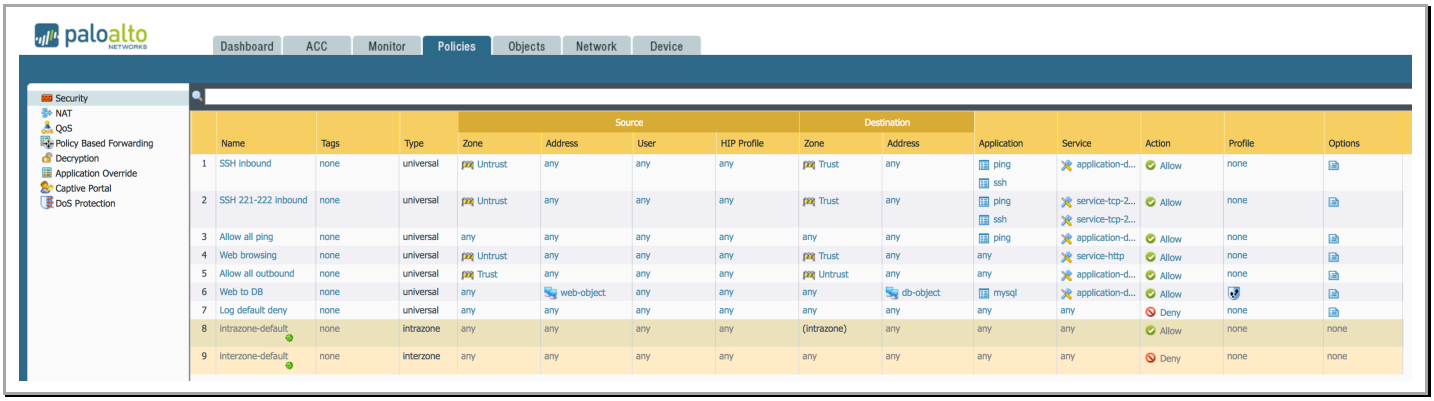
Go to (http://WebserverURL/sql-attack.html) and simulate a web to db ssh attempt by clicking on the **LAUNCH WEB TO DB SSH ATTEMPT.**

This launches a CGI script that attempts to ssh as root to the db server from the web server. Now return to the firewall's monitor tab to note the failed traffic:

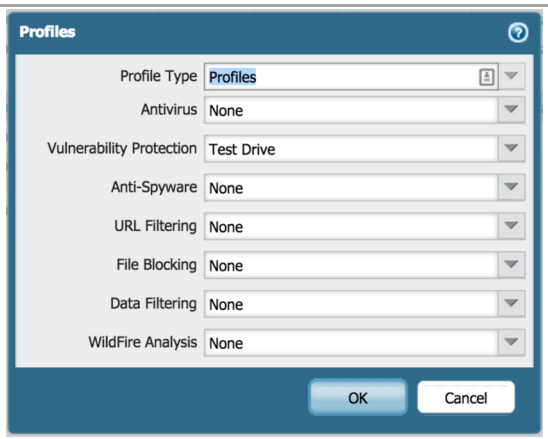


Task 2 – Trigger the SQL brute force attack and review logs

On the firewall's security policies tab, under Security, Rule 6, you will notice that the web to db traffic is protected further by a vulnerability profile:



Now click on the icon in the Profile column and you will see all the threat protection profiles



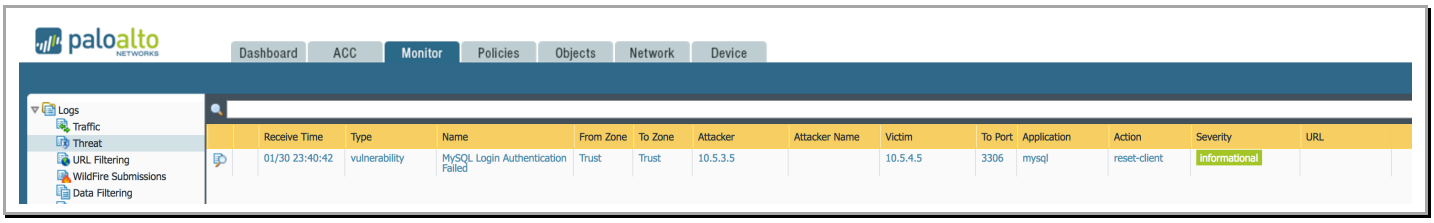
Note the Vulnerability Protection profile. This is a custom profile created just for this lab. It is part of the default vulnerability protection profile but is called out separately for the purpose of this demo environment.

Let's finally trigger the attack. Head back to the sql-attack.html page at (http://WebserverURL/sql-attack.html)

Click on Launch Brute Force Attack to start a script that will generate multiple failed MySQL authentication attempts.

LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING

This will launch some scripted attacks on the SQL server and use the pre-configured threat protection to show and block those attacks on the VM-Series firewall. Now return to the firewall and click the Monitor tab and then click on Threats in the left-hand pane under Logs and notice the new vulnerability log message regarding the failed MySQL events:



The CGI script you launched above attempted to login to the MySQL database multiple times with an incorrect password. The VM-Series firewall saw this activity and using the vulnerability profile, reset the connection and logged the activity.

7. Cleanup

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