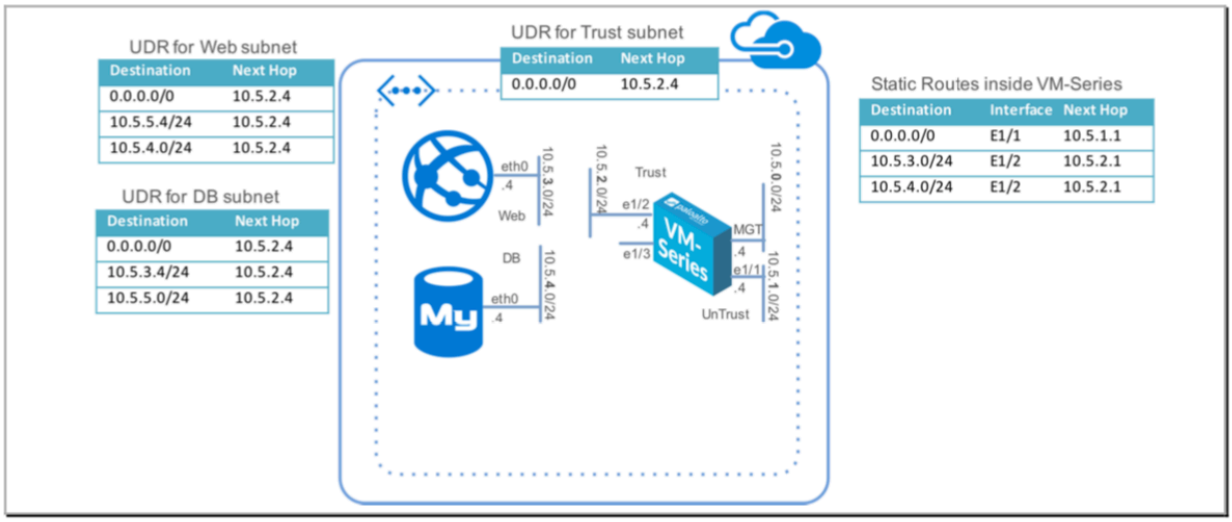
Azure Resource Manager Template

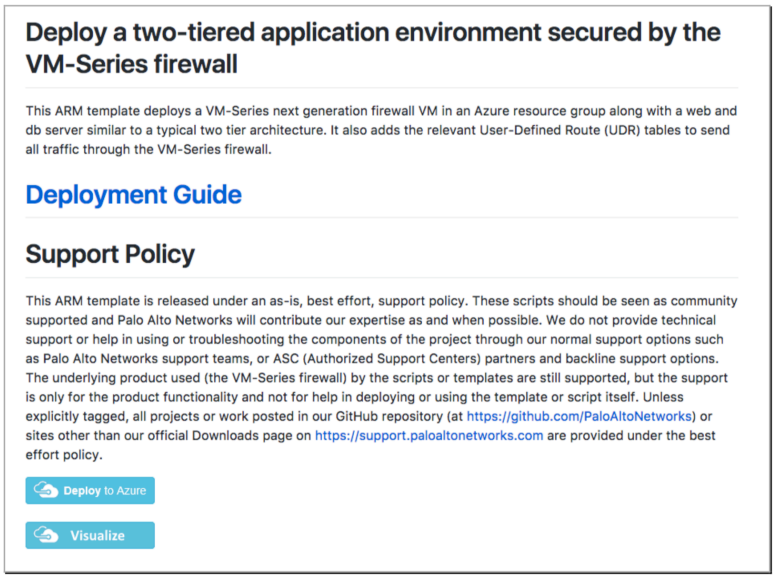
Step 1



Step 2

The below **Deploy to Azure** button embeds an Azure ARM

https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample



Deploy a two-tiered application environment secured by the VM-Series firewall

This ARM template deploys a VM-Series next generation firewall VM in an Azure resource group along with a web and db server similar to a typical two tier architecture. It also adds the relevant User-Defined Route (UDR) tables to send all traffic through the VM-Series firewall.

Deployment Guide

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.

Deploy to Azure

Visualize

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.

Before, select the option: Edit template

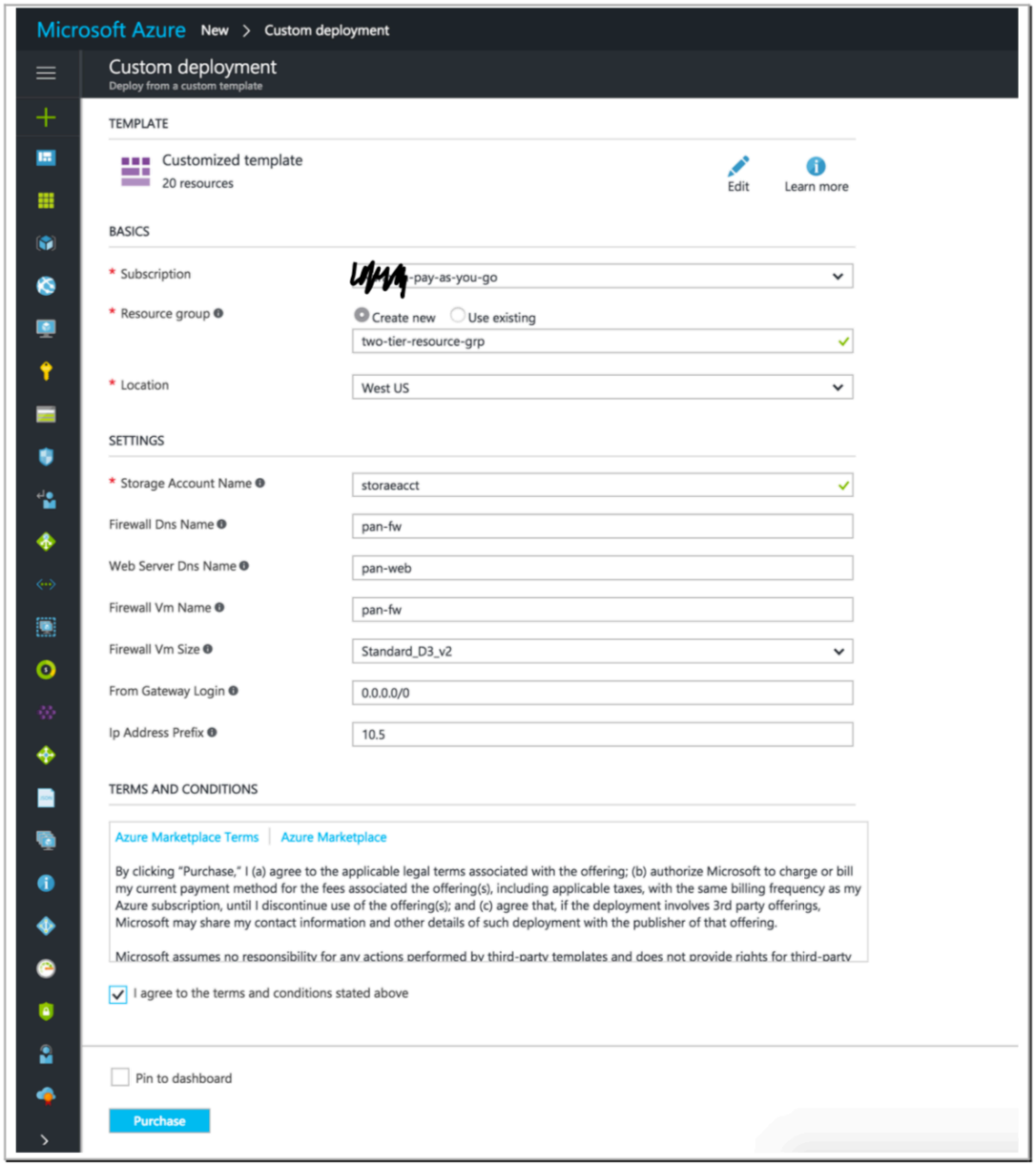
Will open a text editor with the son file. Look for the following line and change the parameter gvmSize as follows:

"gvmSize": “Standard_B1ls",

Click Save, then fill the requested information as follows:

Resource Group: username, E,g: lcastrose

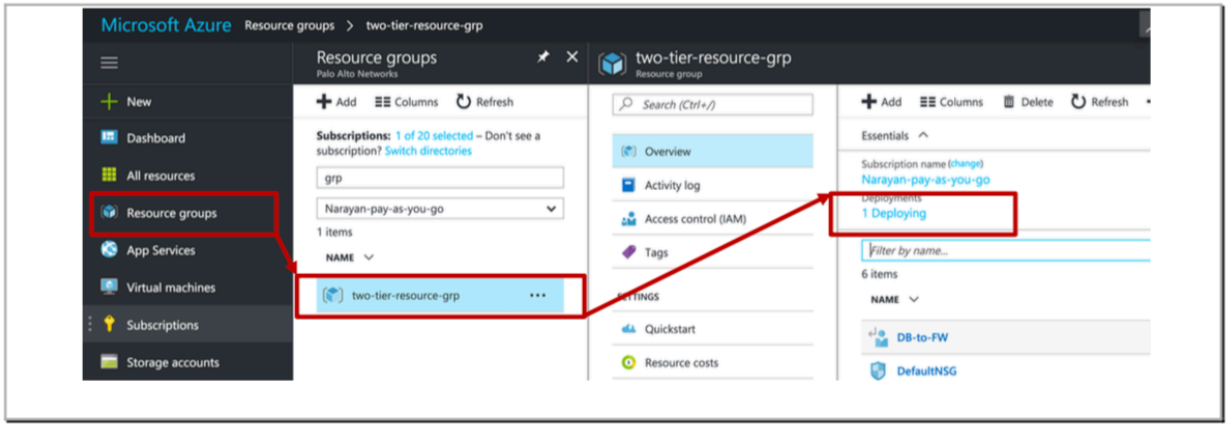
Storage Account Name: username, E.g: lcastrose

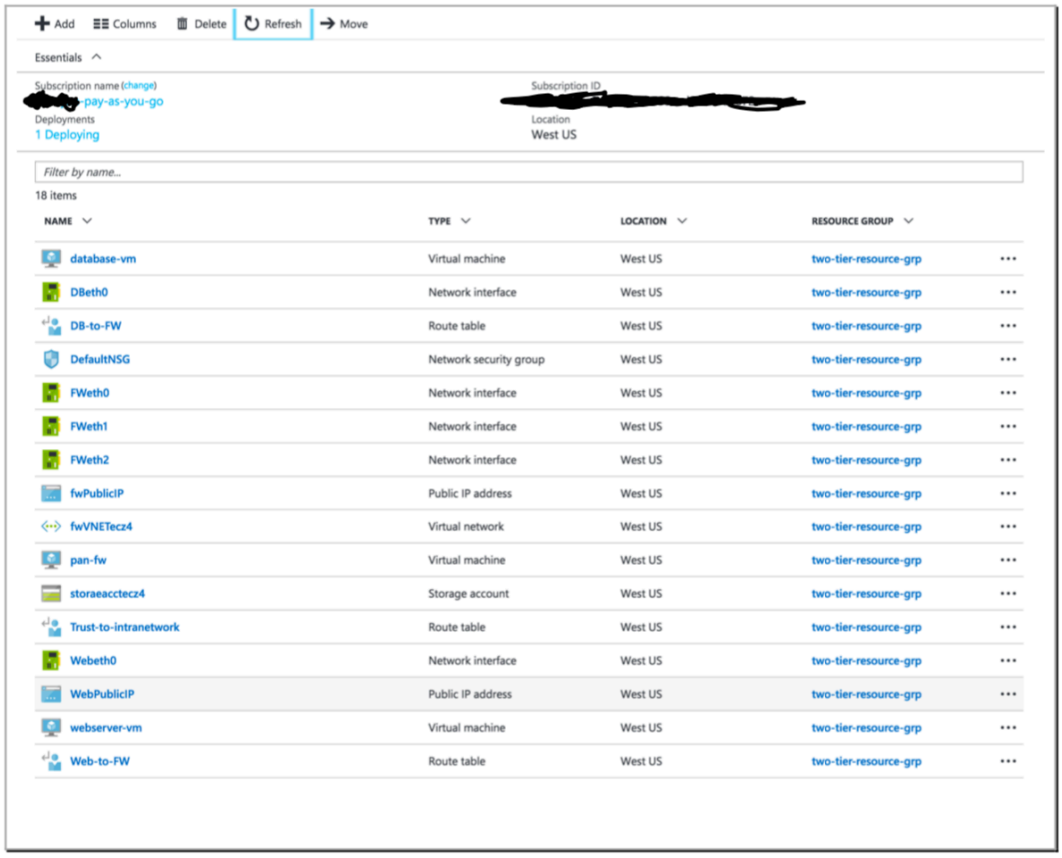


Step 3

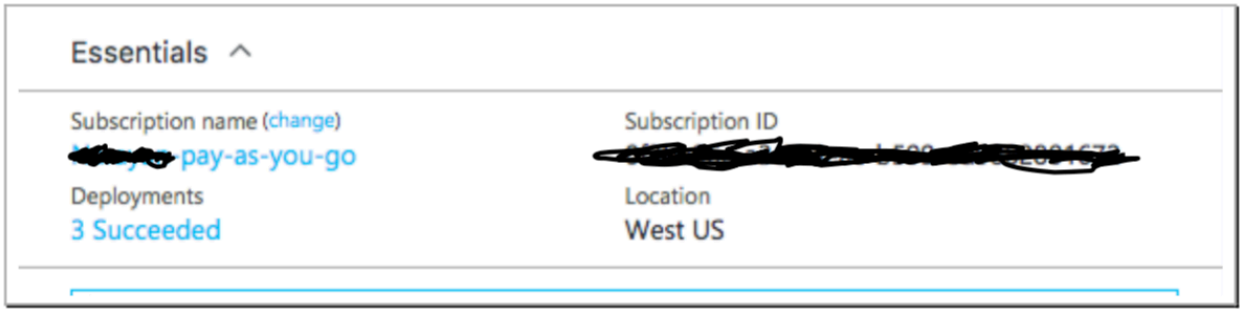
Check Deployment Status

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.





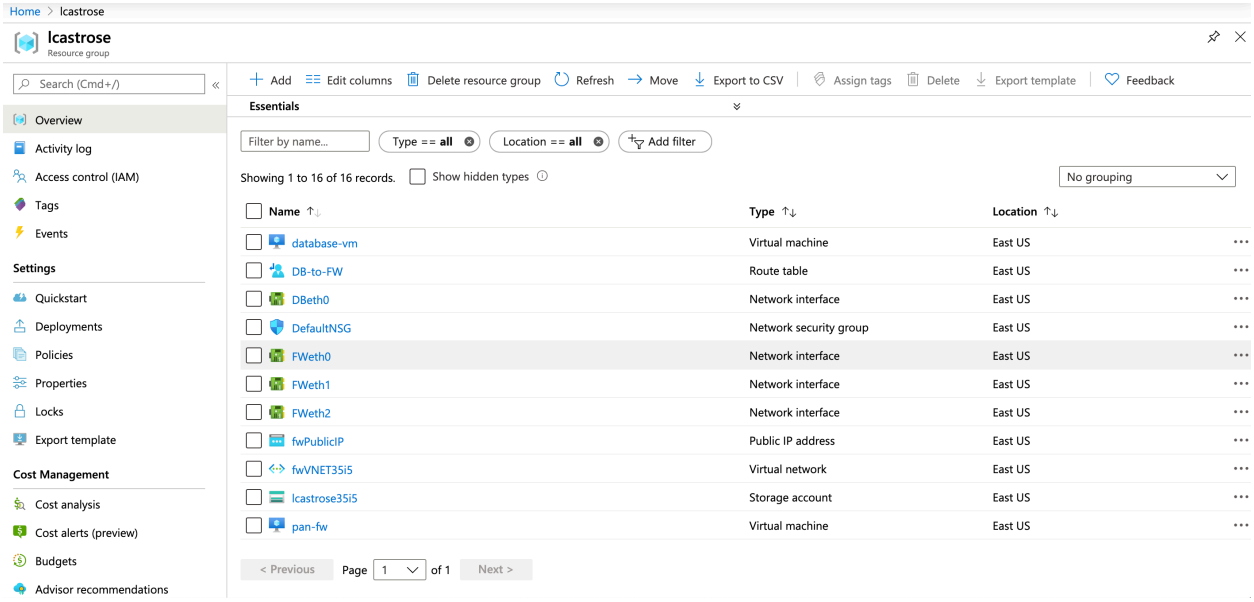
If the ARM template deployment was successful, the deployment state will show as “3 Succeeded”



Step 4

Review the Provisioned Resources

Verify that the resources match this topology.



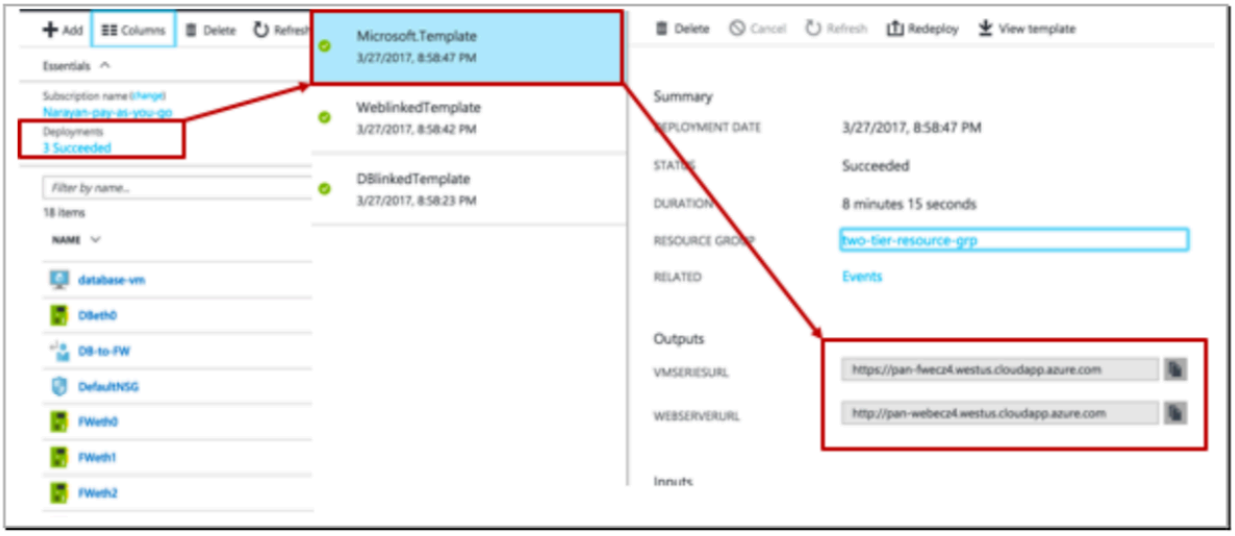
Step 5

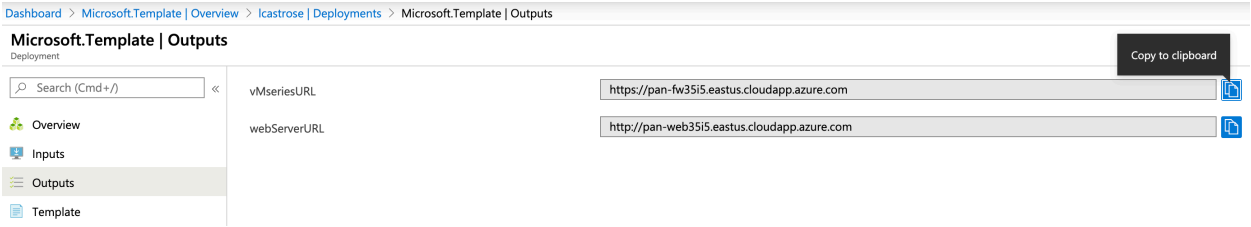
PanOS UI

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

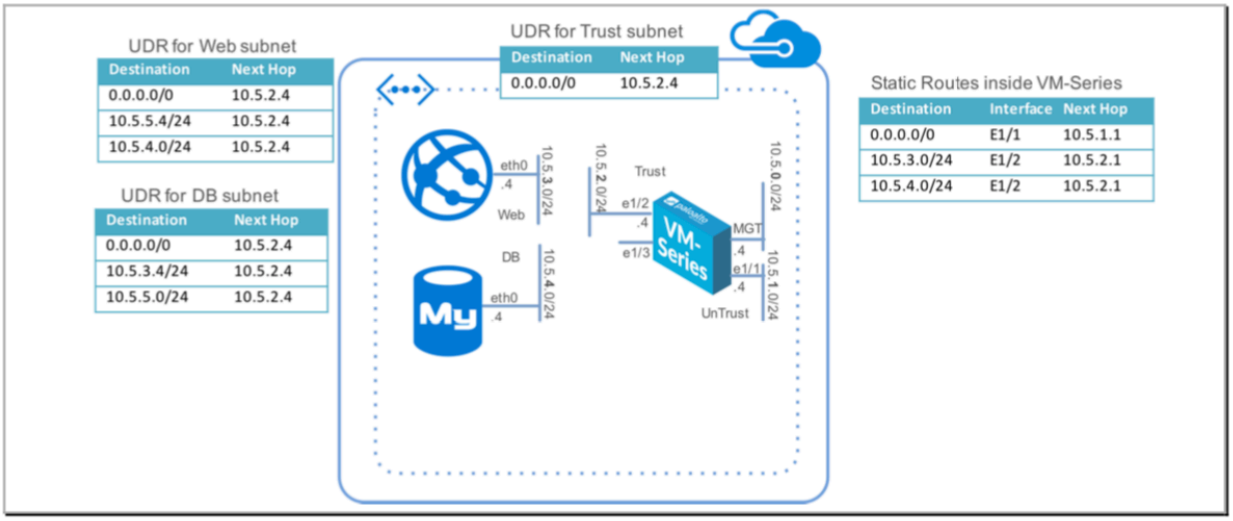
To access the firewall login page, access the URL from the azure portal template deployment summary page.

You should be able to log into the VMSeriesURL using the username/password: paloalto/ Pal0Alt0@123





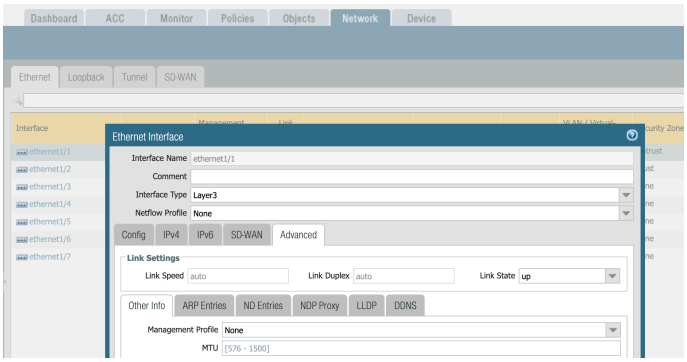
Step 6 - Networking



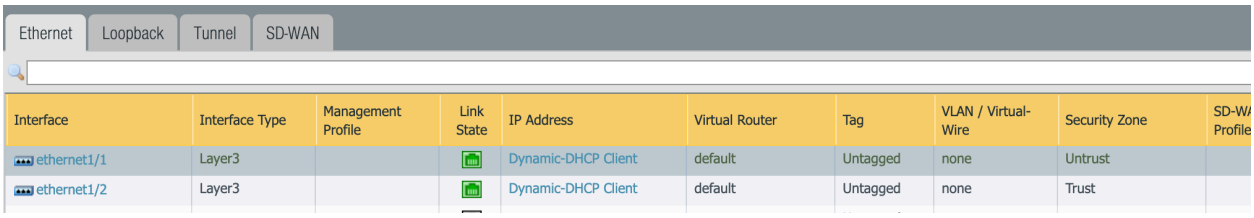
The interface (Ethernet 1/1) in the Unturst zone is the interface that is exposed to the outside world. All traffic enters through this interface.

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).

NOTE: Go the Network and set both E1/1 and E1/2 interfaces to UP, then click Commit



Then validate both interfaces are up “green”



Step 7

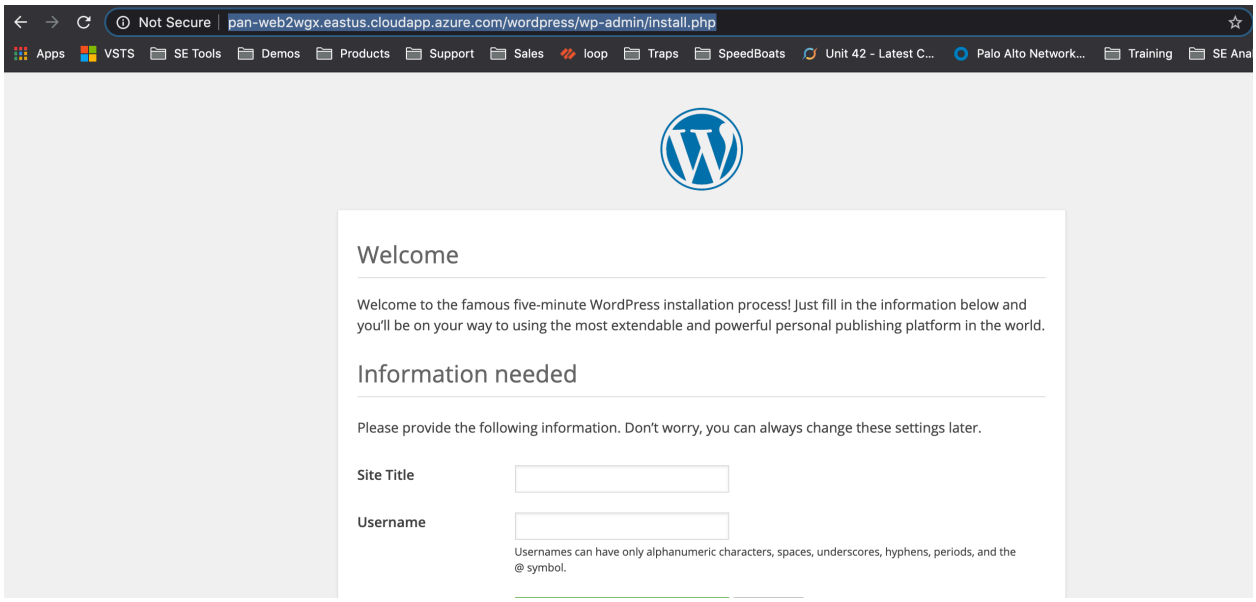
Verify Static Content on Web Server

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

Go to the Wordpress Server

Add the following string at the end of the second URL from the deployment:

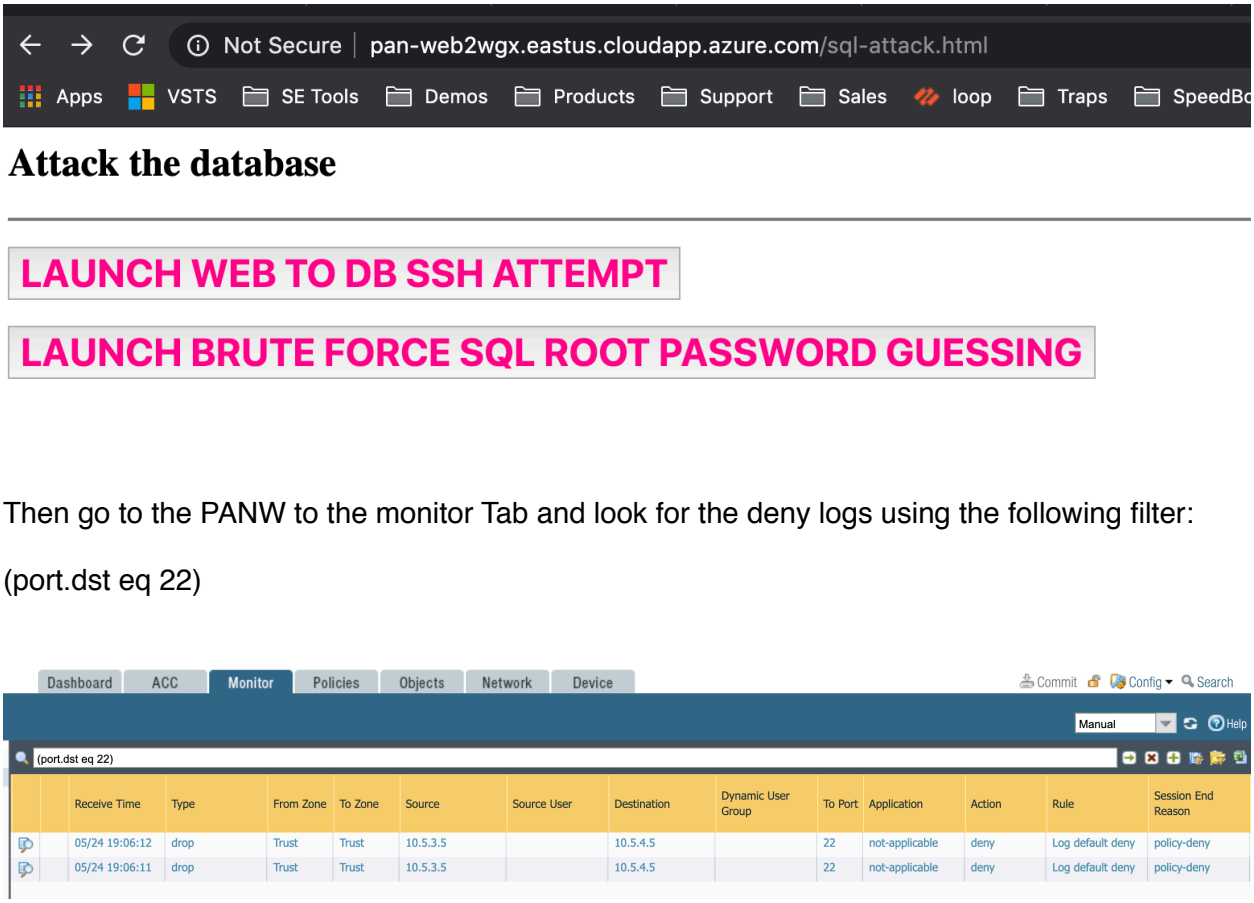
<http://pan-web2wgx.eastus.cloudapp.azure.com>/wordpress



Step 8 - Simulate attacks to the web server

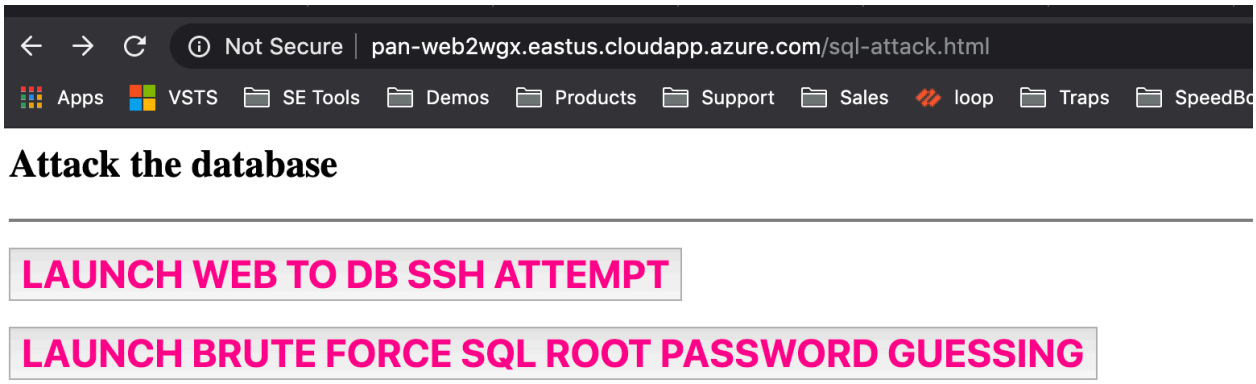
<http://pan-web2wgx.eastus.cloudapp.azure.com>/sql-attack.html

Click on Launch Web to DB SSH Attempt, to simulate East-West Traffic



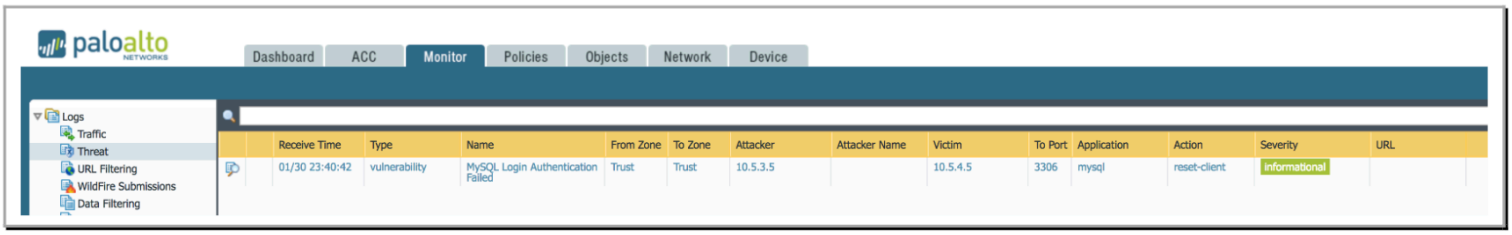
Step 9 - Simulate Brute Force attack

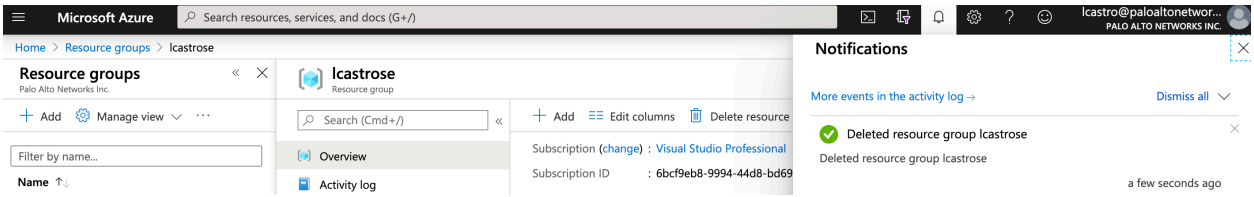
Go back and click on Launch Brute Force SQL Root Password Guessing



Upgrade the Threat and Applications from Dynamic Updates.

Go to the PANW Monitor Tab on Threat Log



Step 10 - Cleanup

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