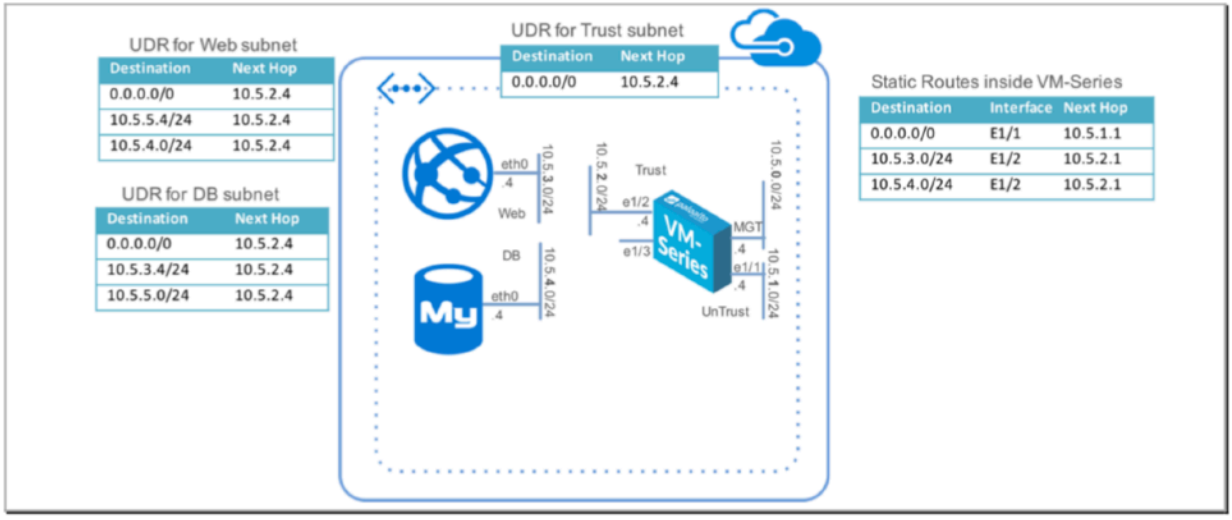
Azure Resource Manager Template

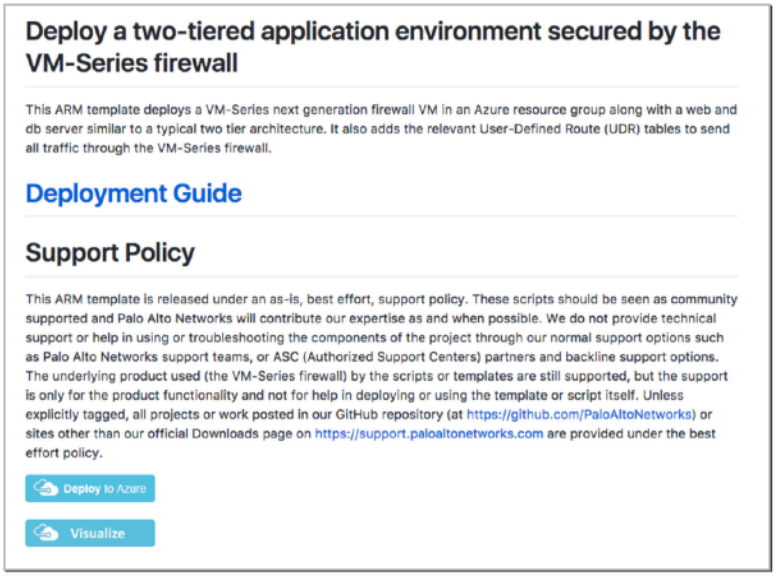
Step 1



Step 2

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

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

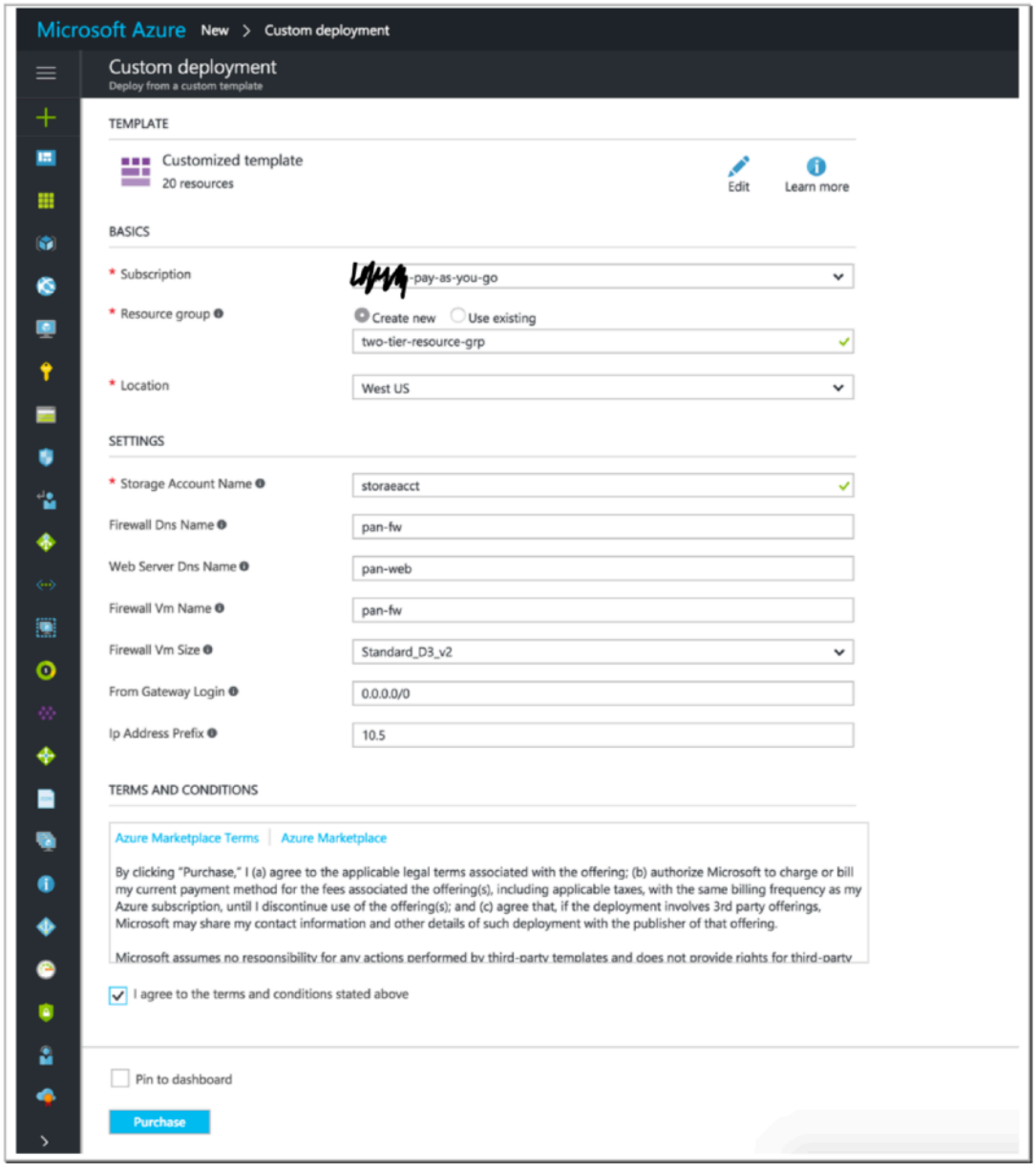


Click “Visualize” for a visual representation of the various resources the template launches. Click “Deploy to Azure” link. You will be prompted to log in to your Azure account and prompted to specify some template parameters.

Create the following

Resource Group: username, E,g: lcastrose

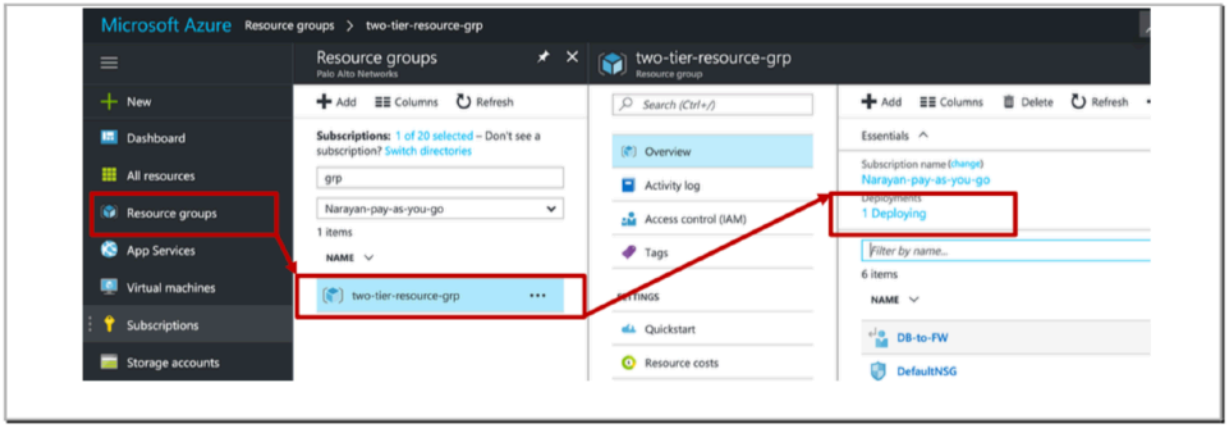
Storage Account Name: username, E.g: lcastrose

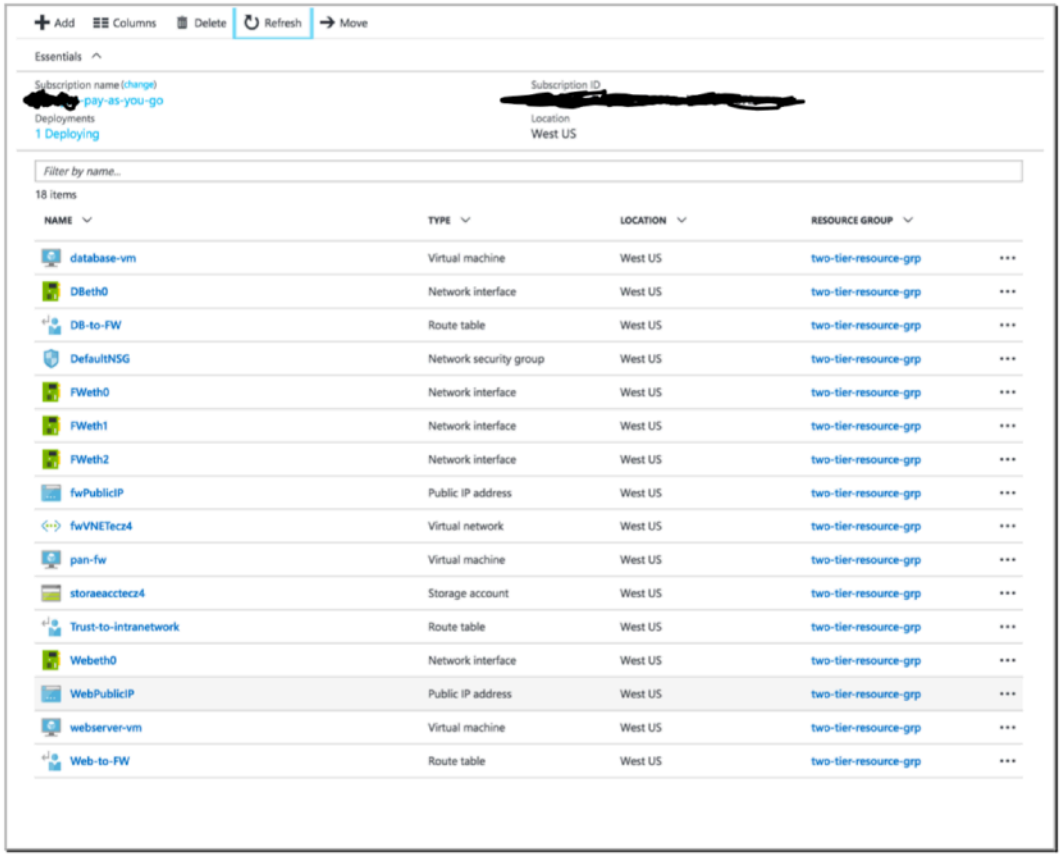


Step 3

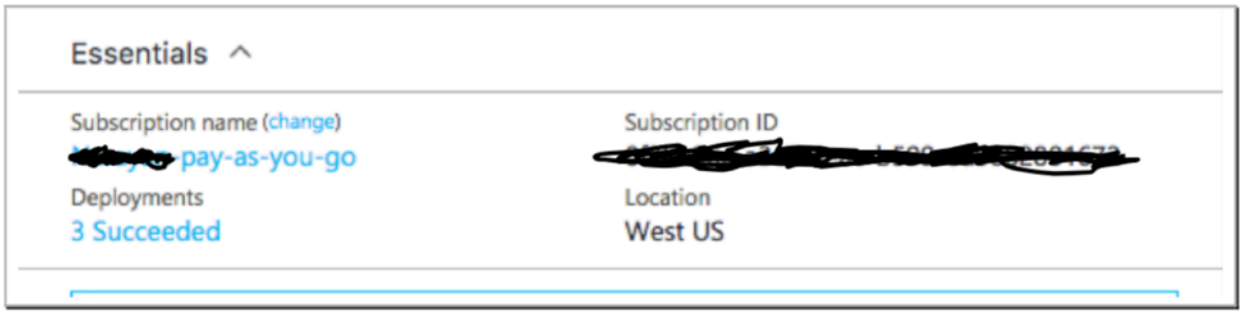
Check Deployment Status

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.





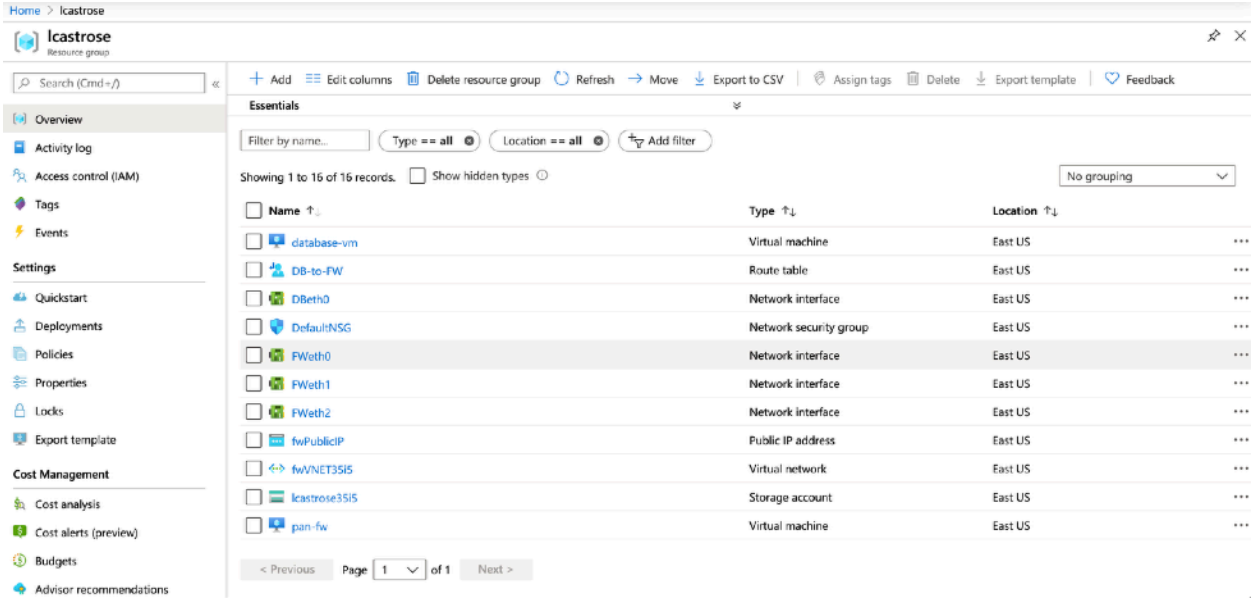
If the ARM template deployment was successful, the deployment state will show as “3 Succeeded”



Step 4

Review the Provisioned Resources

Verify that the resources match this topology.



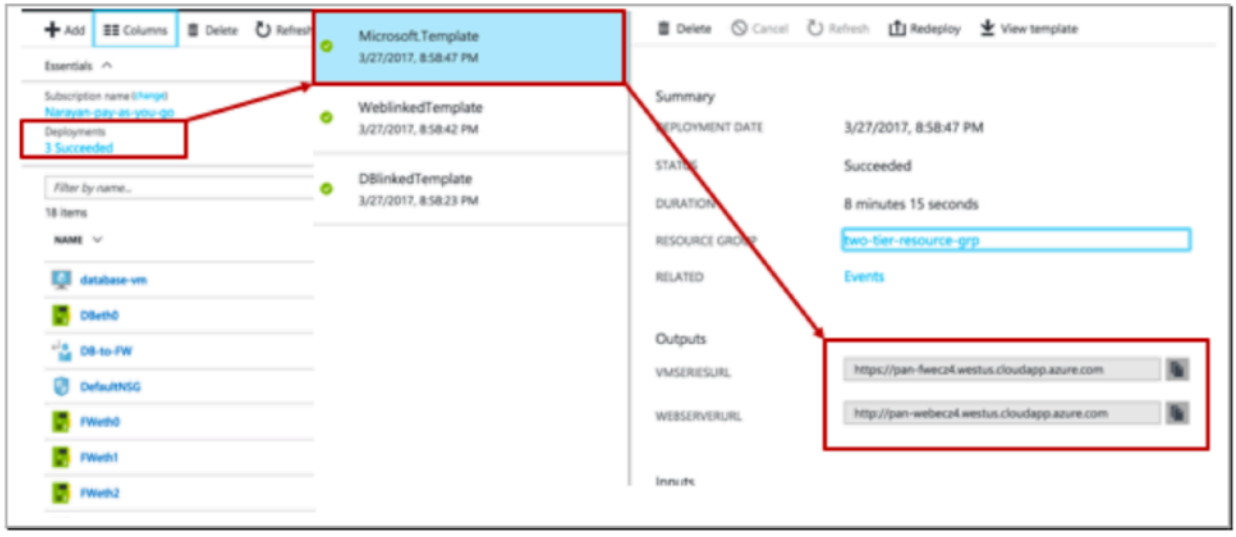
Step 5

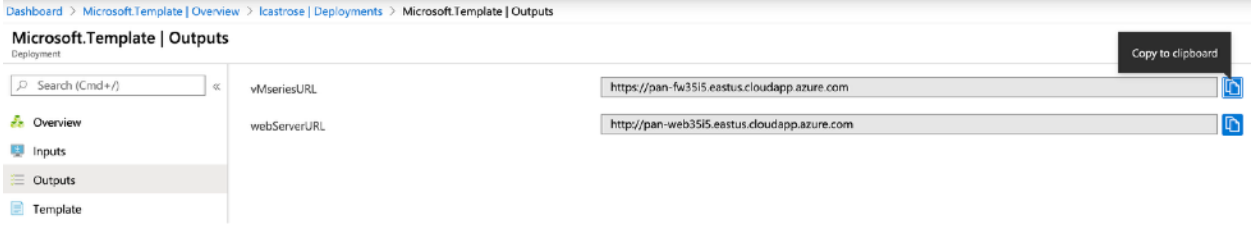
PanOS UI

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

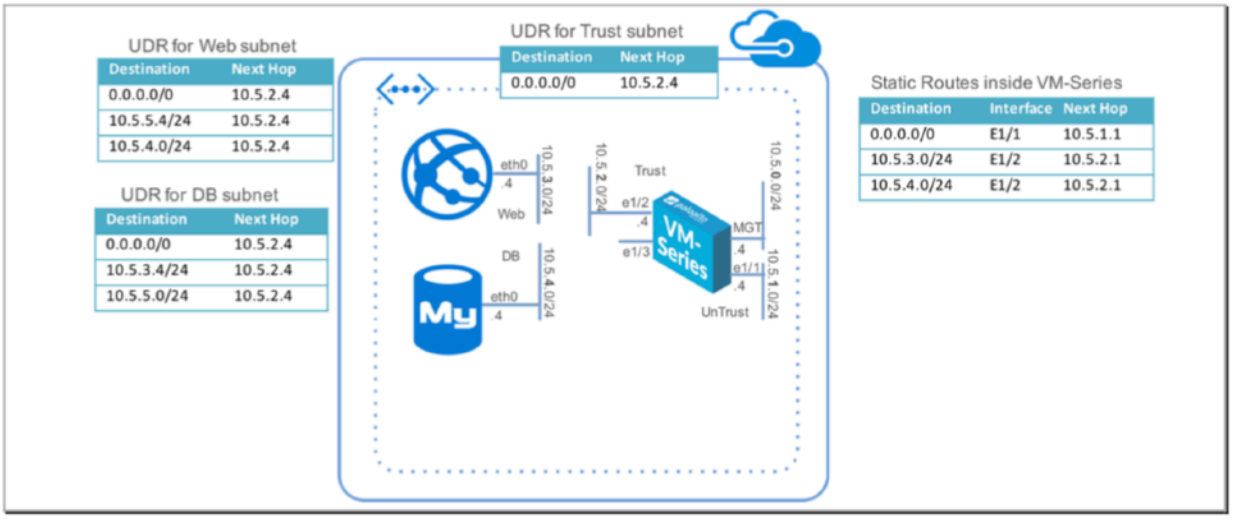
To access the firewall login page, access the URL from the azure portal template deployment summary page.

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





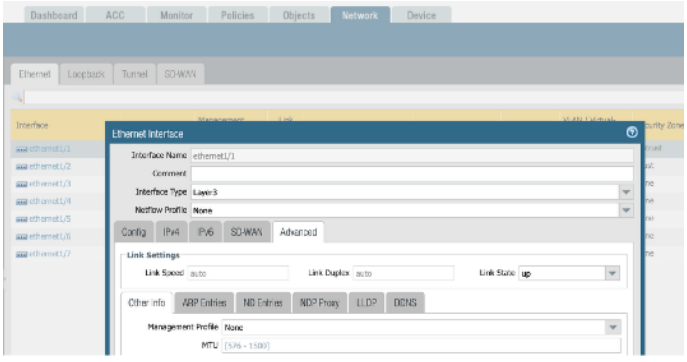
Step 6 - Networking



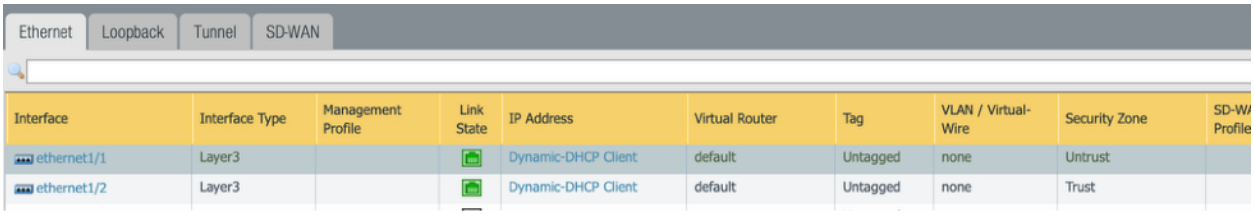
The interface (Ethernet 1/1) in the Unturst zone is the interface that is exposed to the outside world. All traffic enters through this interface.

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

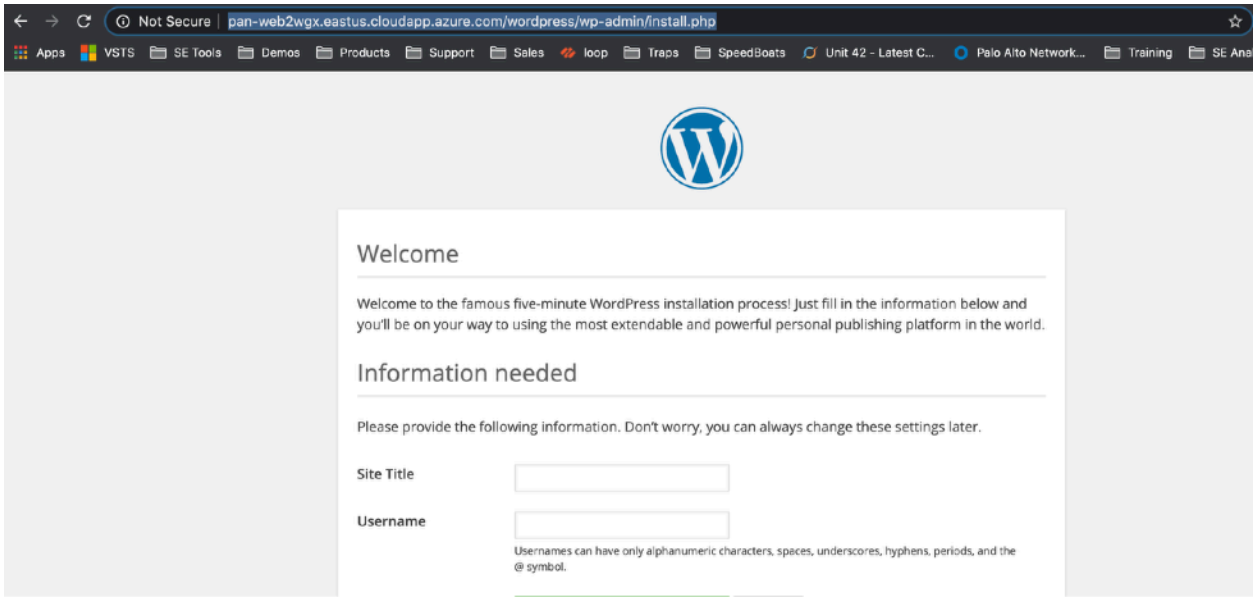
Verify Static Content on Web Server

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:

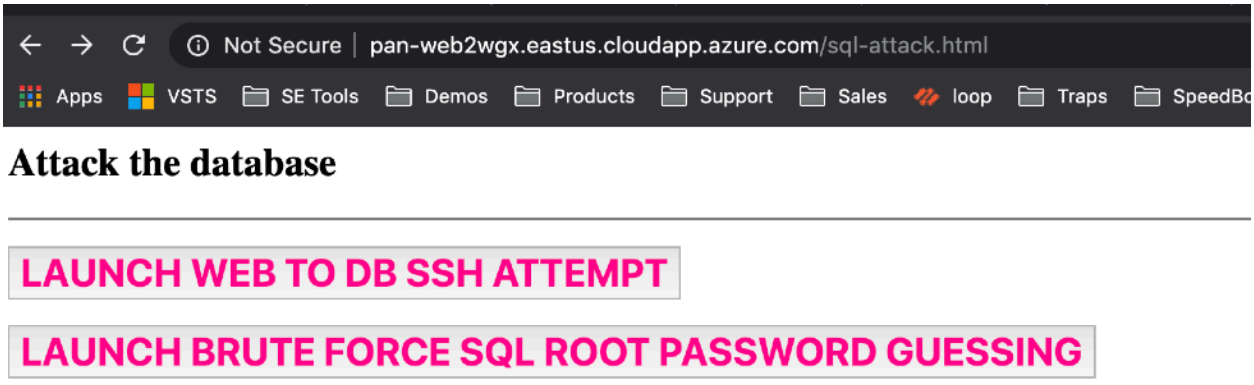
<http://pan-web2wgx.eastus.cloudapp.azure.com>/wordpress



Step 8 - Simulate attacks to the web server

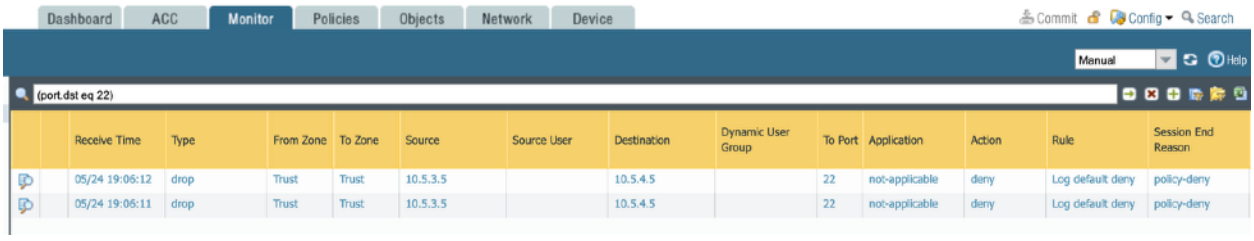
<http://pan-web2wgx.eastus.cloudapp.azure.com>/sql-attack.html

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



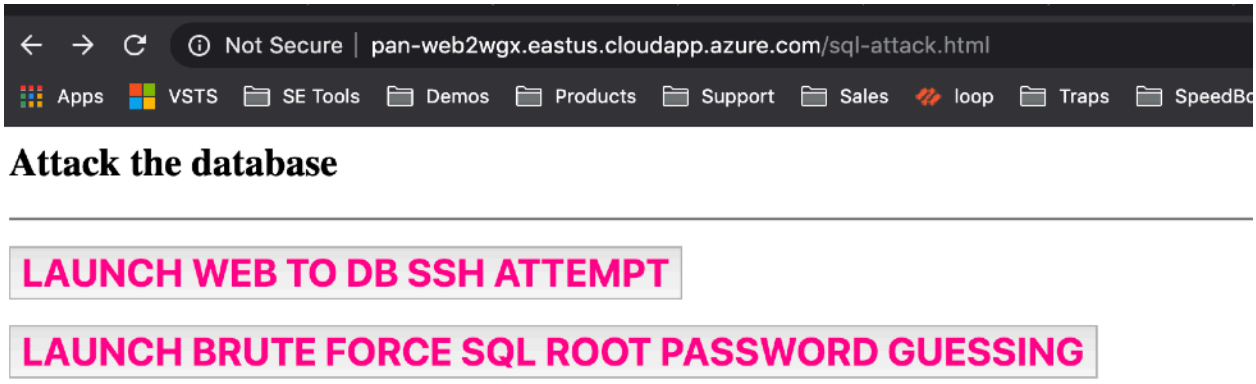
Then go to the PANW to the monitor Tab and look for the deny logs using the following filter:

(port.dst eq 22)

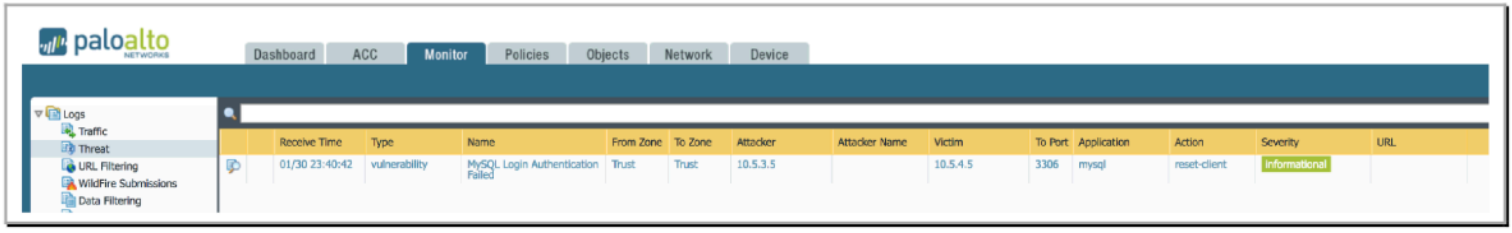


Step 9 - Simulate Brute Force attack

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



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.