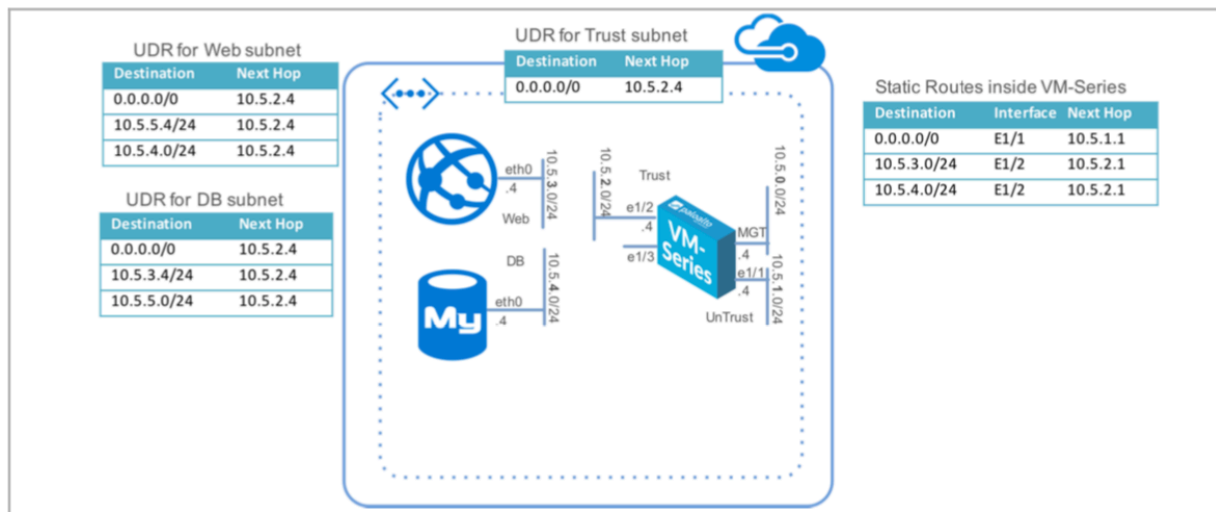


## Azure Resource Manager Template

### 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.

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

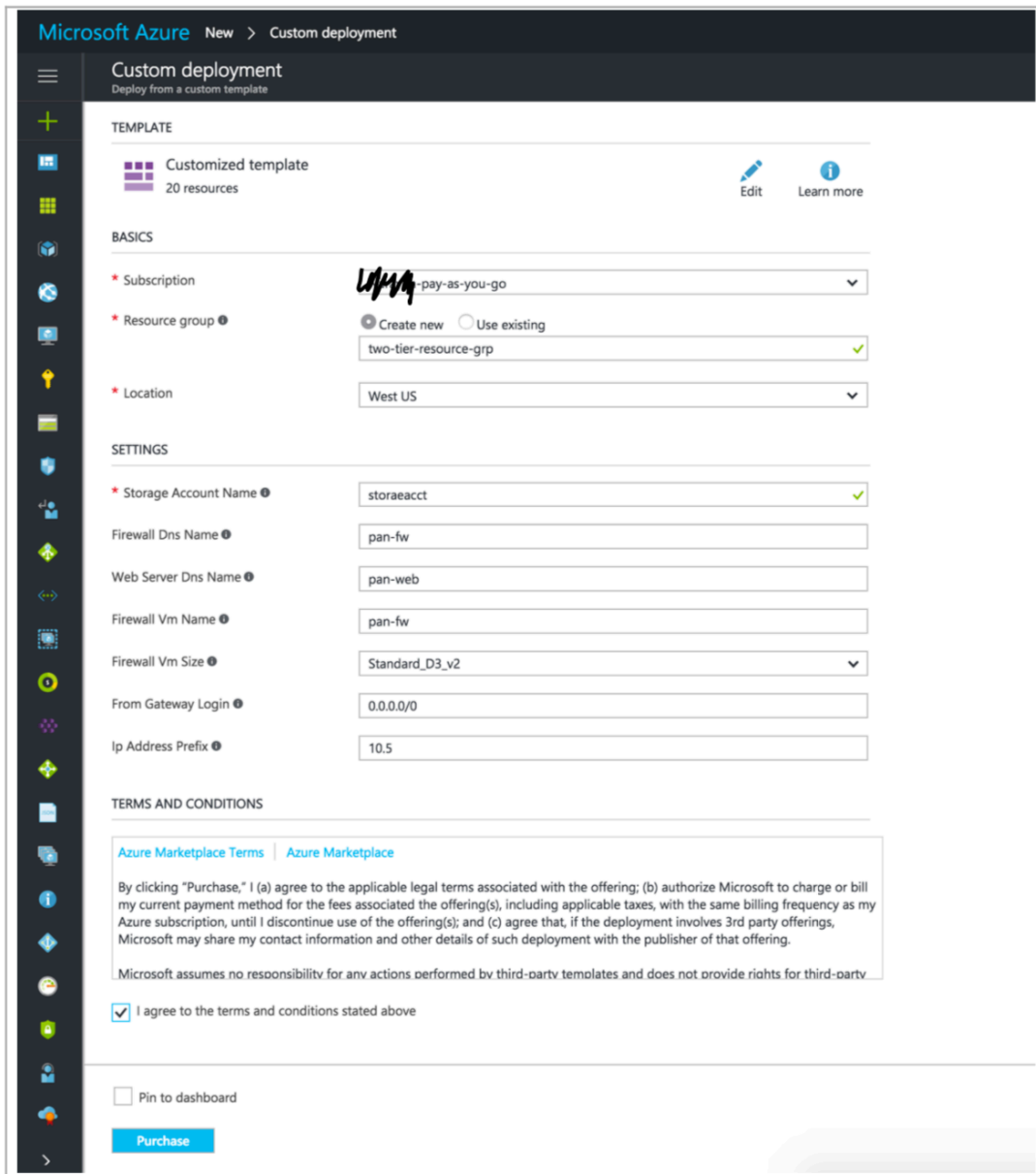
Will open a text editor with the son file. Look for the following line and change the parameter gvmSize as follows:

"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



The screenshot shows the Microsoft Azure Custom deployment portal. The left sidebar contains navigation icons for various Azure services. The main content area is titled "Custom deployment" and "Deploy from a custom template". It is divided into sections: TEMPLATE, BASICS, SETTINGS, and TERMS AND CONDITIONS.

**TEMPLATE**

- Customized template (20 resources)
- Buttons: Edit, Learn more

**BASICS**

- \* Subscription: pay-as-you-go
- \* Resource group: Create new (selected) / Use existing. Value: 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.

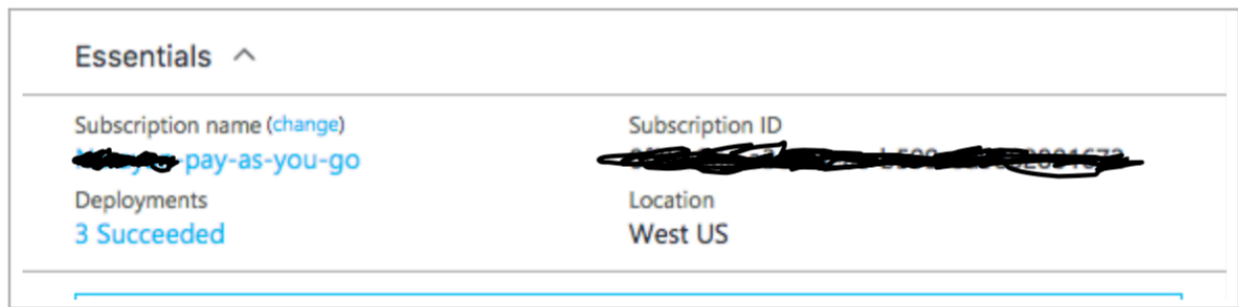
☒ I agree to the terms and conditions stated above

☐ Pin to dashboard

**Purchase**



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.

Home > Icastrose

**Icastrose**  
Resource group

Search (Cmd+/)

+ Add Edit columns Delete resource group Refresh Move Export to CSV Assign tags Delete Export template Feedback

**Essentials**

Filter by name... Type == all Location == all Add filter

Showing 1 to 16 of 16 records. Show hidden types No grouping

Name	Type	Location
database-vm	Virtual machine	East US
DB-to-FW	Route table	East US
DBeth0	Network interface	East US
DefaultNSG	Network security group	East US
FWeth0	Network interface	East US
FWeth1	Network interface	East US
FWeth2	Network interface	East US
fwPublicIP	Public IP address	East US
fwVNET35IS	Virtual network	East US
Icastrose35IS	Storage account	East US
pan-fw	Virtual machine	East US

< Previous Page 1 of 1 Next >

### Step 5

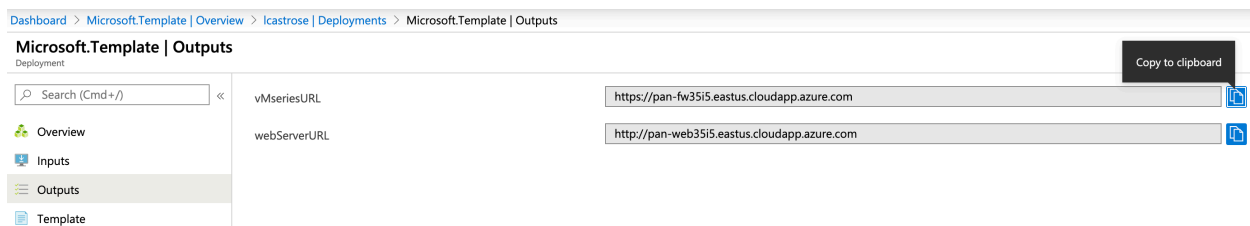
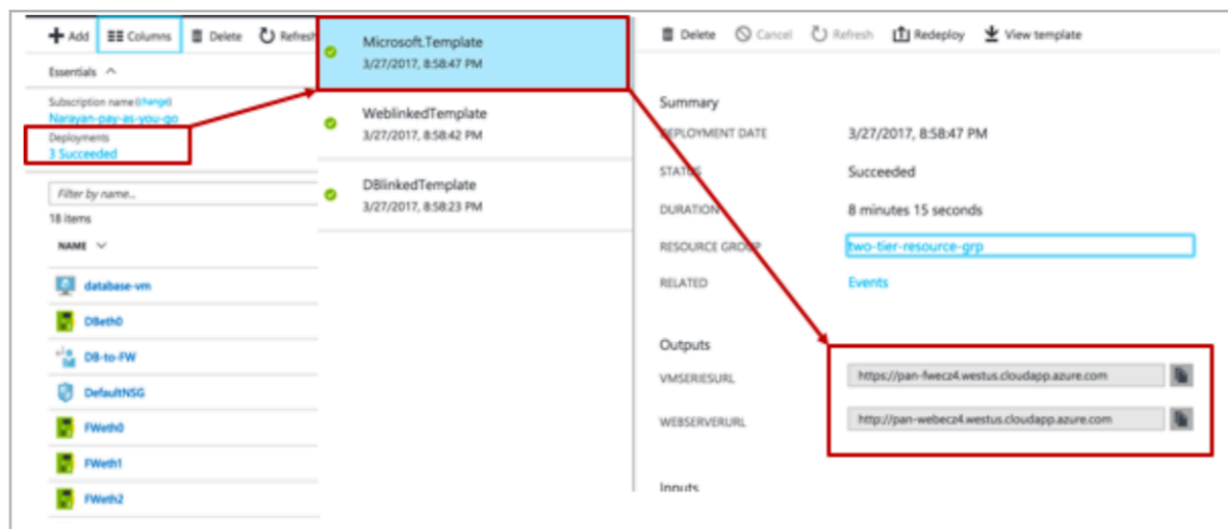
## PanOS UI

## Login to the VM-Series firewall

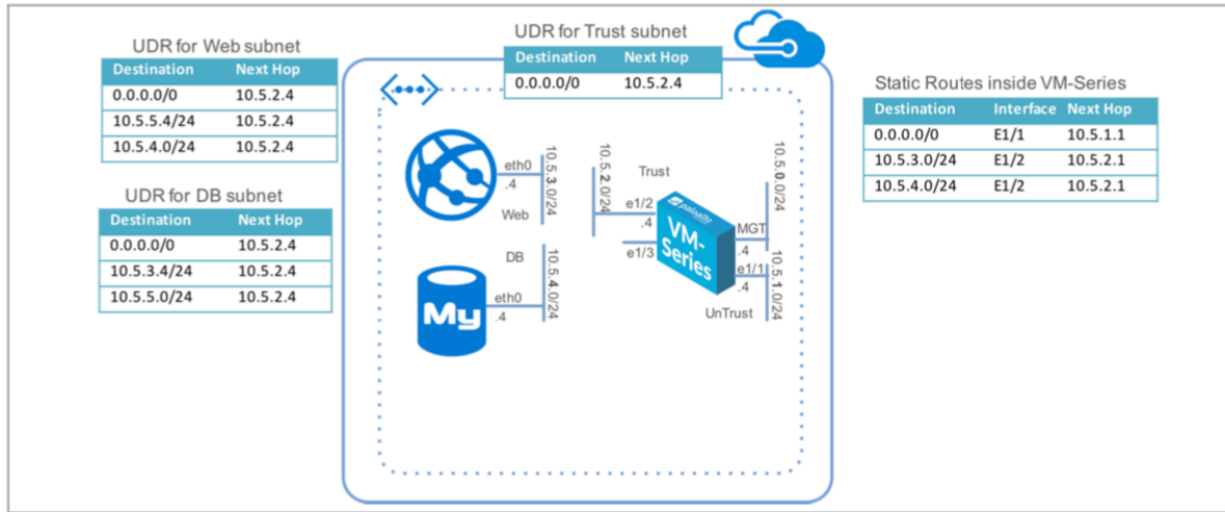
## Review key portions of the firewall configurations

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



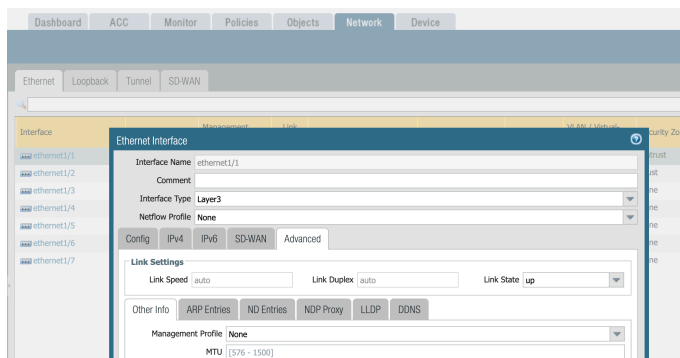
## Step 6 - Networking



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



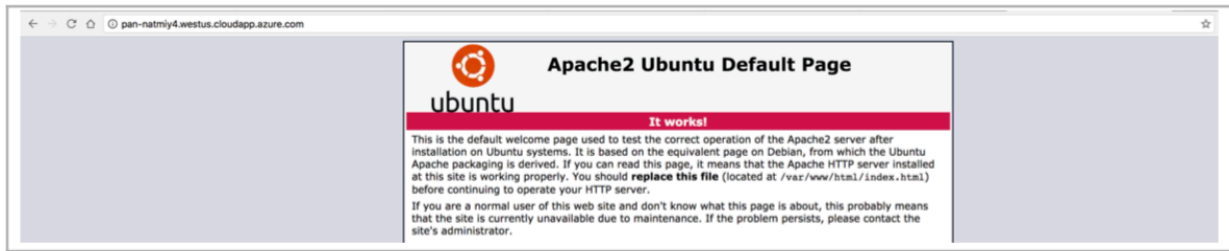
Then validate both interfaces are up “green”

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	SD-W Profile
ethernet1/1	Layer3		🟢	Dynamic-DHCP Client	default	Untagged	none	Untrust	
ethernet1/2	Layer3		🟢	Dynamic-DHCP Client	default	Untagged	none	Trust	

## Step 7

### Verify Static Content on Web Server

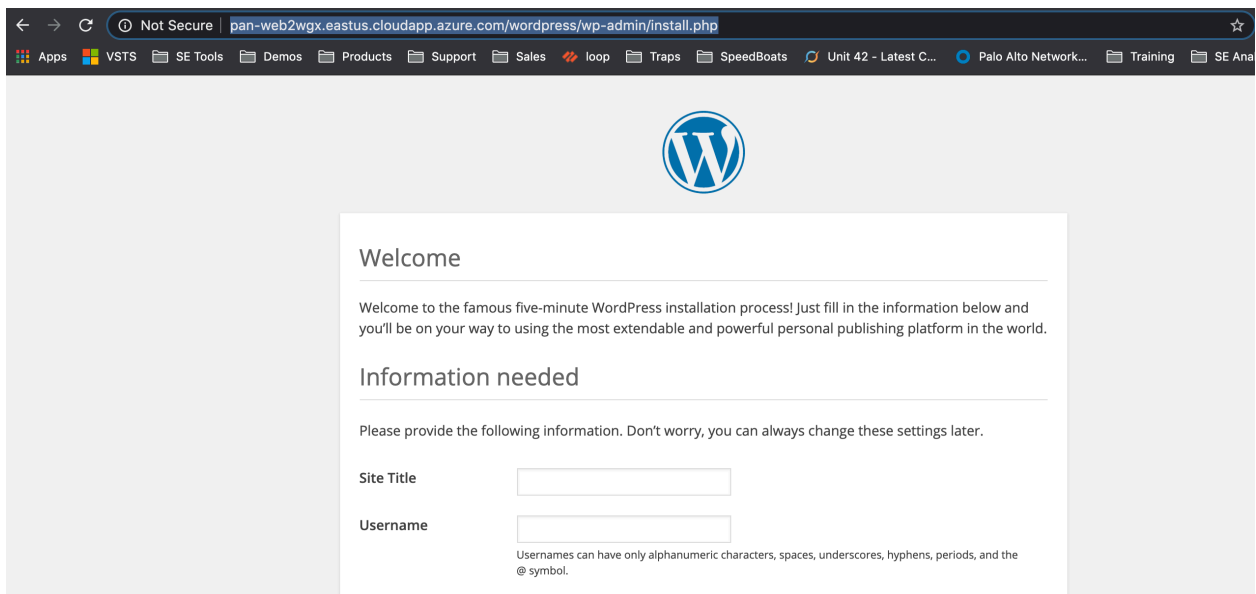
Using the second URL (WebserverURL) in the output section of the deployment summary access the static content of the webserver and you should see:



Go to the Wordpress Server

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

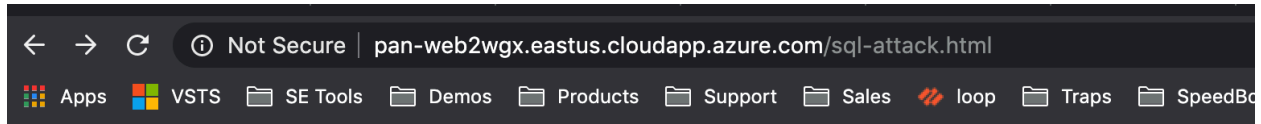
<http://pan-web2wgx.eastus.cloudapp.azure.com/wordpress>



## 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



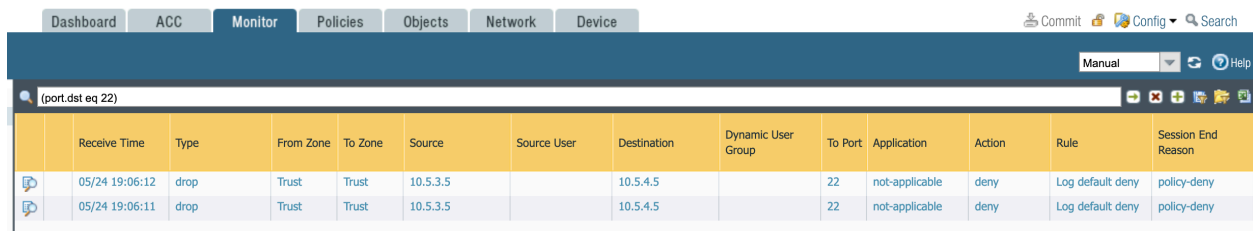
## Attack the database



**LAUNCH WEB TO DB SSH ATTEMPT**

**LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING**

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

(port.dst eq 22)

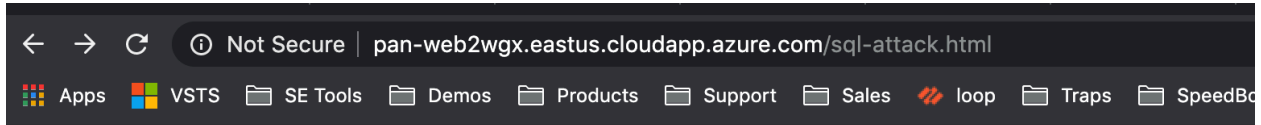


	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	Dynamic User Group	To Port	Application	Action	Rule	Session End Reason
	05/24 19:06:12	drop	Trust	Trust	10.5.3.5		10.5.4.5		22	not-applicable	deny	Log default deny	policy-deny
	05/24 19:06:11	drop	Trust	Trust	10.5.3.5		10.5.4.5		22	not-applicable	deny	Log default deny	policy-deny



## Step 9 - Simulate Brute Force attack

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



## Attack the database

**LAUNCH WEB TO DB SSH ATTEMPT**

**LAUNCH BRUTE FORCE SQL ROOT PASSWORD GUESSING**

Upgrade the Threat and Applications from Dynamic Updates.

Go to the PANW Monitor Tab on Threat Log

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	URL
01/30 23:40:42	vulnerability	MySQL Login Authentication Failed	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	reset-client	informational	

## Step 10 - Cleanup

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

