

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>

Table of Contents

Version History	3
Support Policy	4
1. About ARM Templates	4
2. Prerequisites.....	6
2.1 Create an Azure account	6
2.2 Add a credit card to your Azure account.....	6
3. Launch the ARM Template	7
3.1 Deploy from Github	7
3.2 The Parameters	10
3.3 Agree to terms and Launch.....	12
3.4 Check Deployment Status	12
3. Review the Provisioned Resources.....	14
4. Access the firewall	18
5. Access the Webserver.....	21
6. Launch some attacks.....	23
a. SSH from Web Server to DB Server	23
b. SQL Brute force attack	23
7. Cleanup	25

Version History

Version number	Comments
1.0	Initial GitHub check-in

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/>

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 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

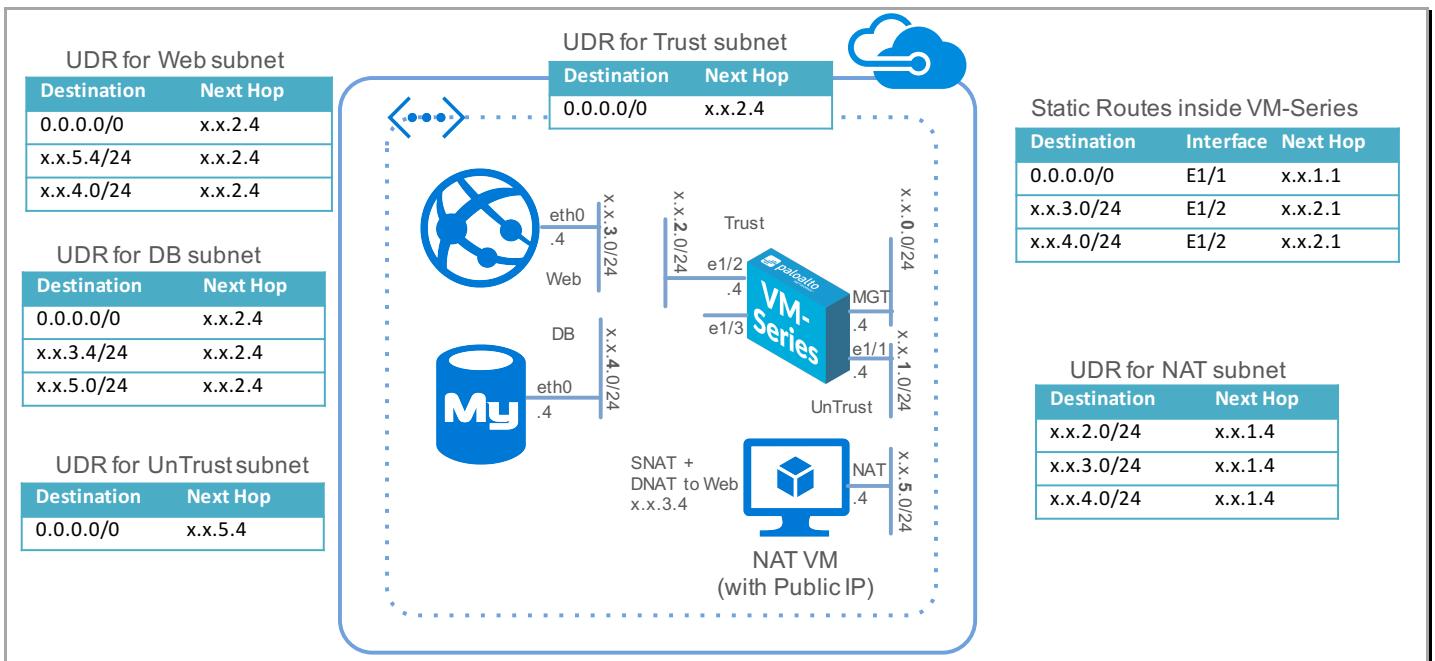
Palo Alto Networks Azure Resource Manager Template Deployment Guide

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>

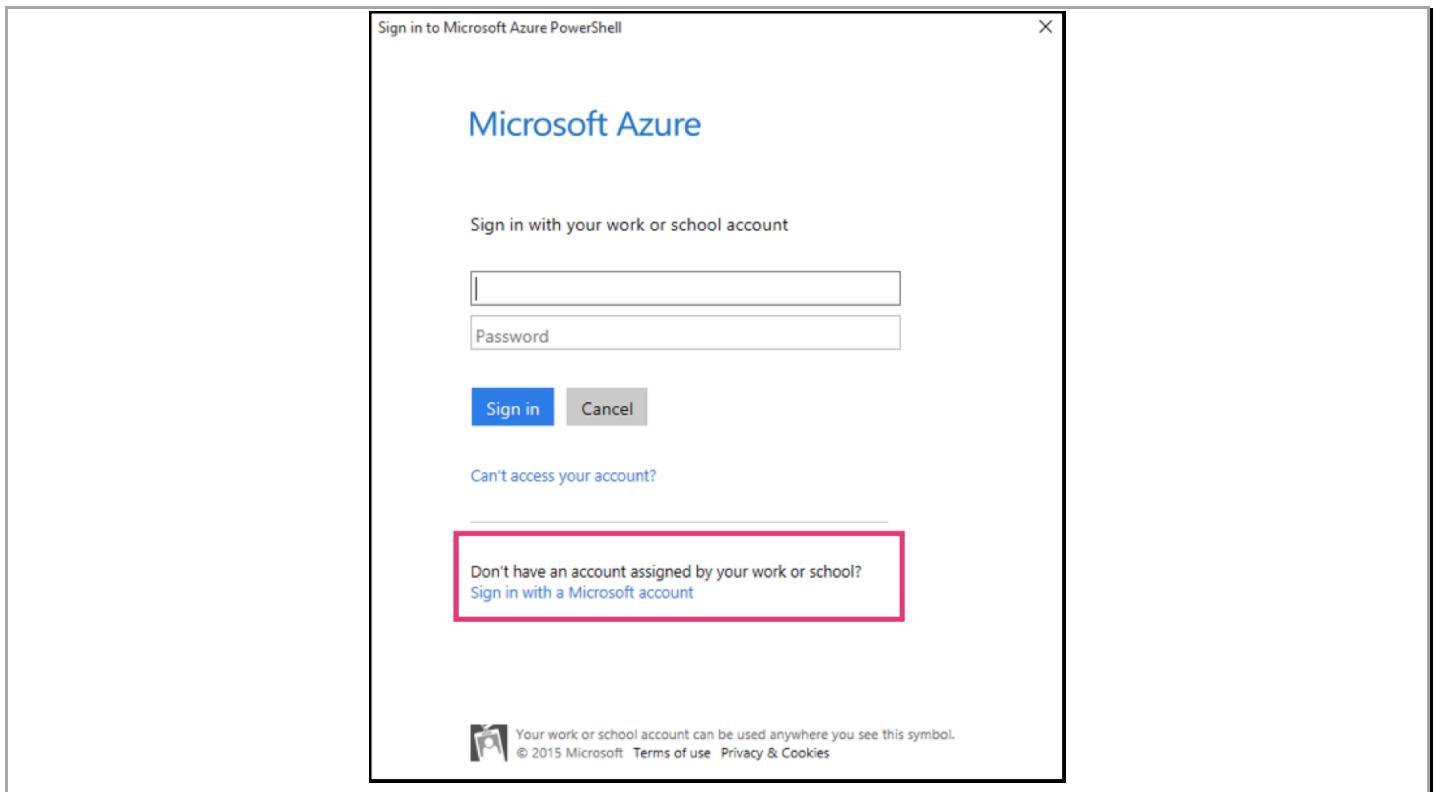
2. Prerequisites

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".



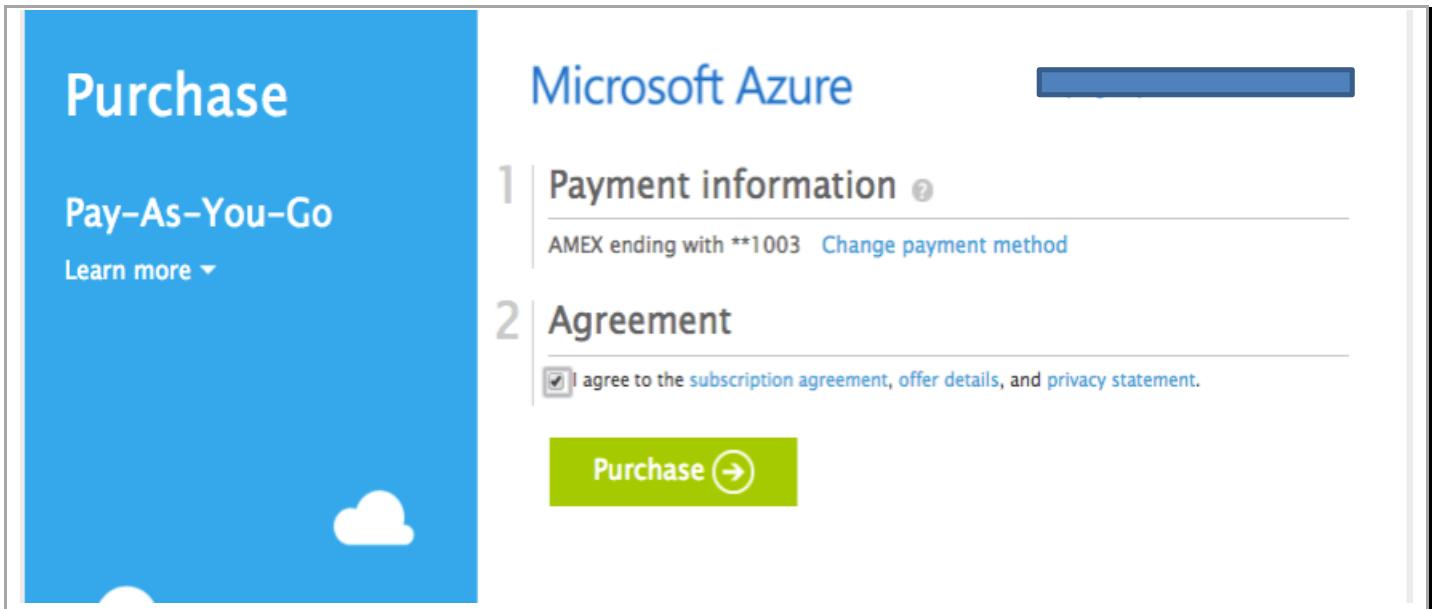
The free trial expires 30 days from account creation date or when \$200 free credits are used up.

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.

VM-Series with NAT VM, and VM's for Web and DB subnet

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.

 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.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

Microsoft Azure New > Custom deployment

Custom deployment
Deploy from a custom template

TEMPLATE

Customized template
25 resources

Edit Learn more

BASICS

* Subscription: **pay-as-you-go**

* Resource group: **Create new** **Use existing**
two-tier-resource-group

* Location: **West US**

SETTINGS

* Storage Account Name: **storageacct**

Firewall Dns Name: **pan-fw**

Nat Dns Name: **pan-nat**

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

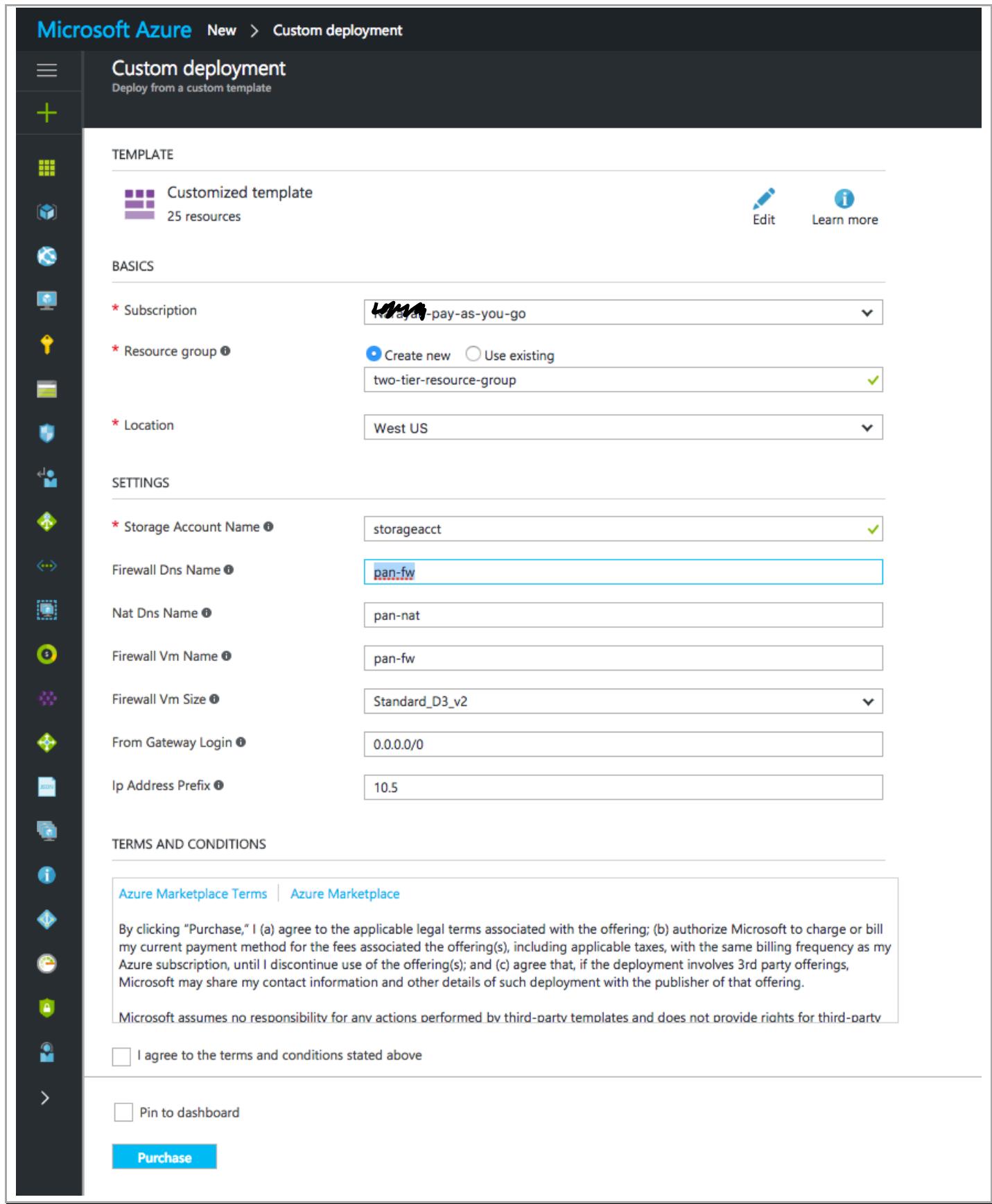
By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until 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

BASICS	
* Subscription	Narayan-pay-as-you-go
* Resource group <small>?</small>	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing two-tier-resource-group
* Location	West US

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

* Storage Account Name <small>?</small>	storageacct
---	-------------

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.

Firewall Dns Name <small>?</small>	pan-fw
------------------------------------	--------

NAT DNS Name:

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.

Nat Dns Name ⓘ	pan-nat
----------------	---------

Firewall VM Name:

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

Firewall Vm Name ⓘ	pan-fw
--------------------	--------

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/>

Firewall Vm Size ⓘ	<input checked="" type="checkbox"/> Standard_D3_v2 <input type="checkbox"/> Standard_D4_v2
--------------------	---

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.

From Gateway Login ⓘ	0.0.0.0/0
----------------------	-----------

IP Address Prefix:

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

Ip Address Prefix ⓘ	10.5
---------------------	------

3.3 Agree to terms and Launch

Agree to the terms and click “Purchase”

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

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.

Microsoft Azure Resource groups > two-tier-resource-group

Resource groups

Subscriptions: 1 of 20 selected – Don't see a subscription? Switch directories

two
Narayan-pay-as-you-go

1 items

NAME

two-tier-resource-group ...

two-tier-resource-group

Overview

Activity log

Access control (IAM)

Tags

SETTINGS

Quickstart

Resource costs

Deployments

Properties

Locks

Essentials

Subscription name (change)
Narayan-pay-as-you-go

Deployments
1 Deploying

Filter by name...

DB-to-FW
DefaultNSG
fwPublicIP
FWUntrust-to-NAT
natPublicIP
NAT-to-FW

Palo Alto Networks Azure Resource Manager Template Deployment Guide

 database-vm	Virtual machine	West US	two-tier-resou...	...
 db-vm-customscript	Microsoft.Com...	West US	two-tier-resou...	...
 DBeth0	Network interf...	West US	two-tier-resou...	...
 DB-to-FW	Route table	West US	two-tier-resou...	...
 DefaultNSG	Network securi...	West US	two-tier-resou...	...
 FWeth0	Network interf...	West US	two-tier-resou...	...
 FWeth1	Network interf...	West US	two-tier-resou...	...
 FWeth2	Network interf...	West US	two-tier-resou...	...
 fwPublicIP	Public IP address	West US	two-tier-resou...	...
 FWUntrust-to-NAT	Route table	West US	two-tier-resou...	...
 fwVNETmiy4	Virtual network	West US	two-tier-resou...	...
 NATeth0	Network interf...	West US	two-tier-resou...	...
 natPublicIP	Public IP address	West US	two-tier-resou...	...

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

Essentials ^

Subscription name ([change](#))
 pay-as-you-go

Subscription ID


Deployments

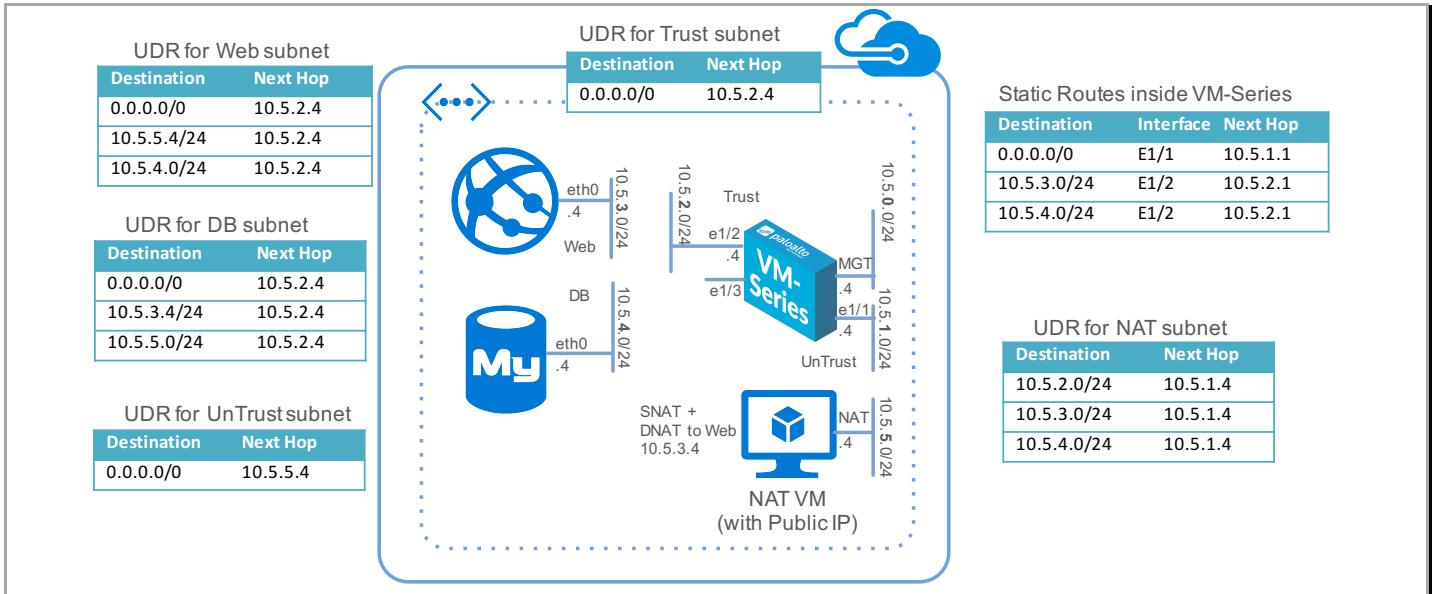
Location

[3 Succeeded](#)

West US

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

database-vm	Virtual machine	West US	two-tier-resou...	***
nat-vm	Virtual machine	West US	two-tier-resou...	***
pan-fw	Virtual machine	West US	two-tier-resou...	***
webserver-vm	Virtual machine	West US	two-tier-resou...	***

Network interfaces

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

 DBeth0	Network interf...	West US	two-tier-resou...	...
 FWeth0	Network interf...	West US	two-tier-resou...	...
 FWeth1	Network interf...	West US	two-tier-resou...	...
 FWeth2	Network interf...	West US	two-tier-resou...	...
 NATeth0	Network interf...	West US	two-tier-resou...	...
 Webeth0	Network interf...	West US	two-tier-resou...	...

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.

 DefaultNSG	Network secur...	azuretestnarayanrg	West US	Narayan-pay-as-you... ...
--	------------------	--------------------	---------	------------------------------

Inbound and outbound rules for the DefaultNSG

The screenshot displays two Azure portal pages for a Network Security Group (NSG) named "DefaultNSG".

DefaultNSG - Inbound security rules:

- Left sidebar:** Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS, Inbound security rules.
- Table:**| PRIORITY | NAME | SOURCE | DESTINATI... | SERVICE | ACTION |
| --- | --- | --- | --- | --- | --- |
| 100 | Allow-Outside-From-IP | 0.0.0.0/0 | Any | Custom (Any/Any) | Allow |
| 101 | Allow-Intra | 10.5.0.0/16 | Any | Custom (Any/Any) | Allow |
| 200 | Default-Deny | Any | Any | Custom (Any/Any) | Deny |
| 65000 | AllowVnetInBound | VirtualNetwork | VirtualN... | Custom (Any/Any) | Allow |
| 65001 | AllowAzureLoadBalancerInBound | AzureLoadBalancer | Any | Custom (Any/Any) | Allow |
| 65500 | DenyAllInBound | Any | Any | Custom (Any/Any) | Deny |

+ Add <> Default rules

Search inbound security rules

User defined Routes (UDRs)

 DB-to-FW	Route table	West US	two-tier-resou... ...
 FWUntrust-to-NAT	Route table	West US	two-tier-resou... ...
 NAT-to-FW	Route table	West US	two-tier-resou... ...
 Trust-to-intranetwork	Route table	West US	two-tier-resou... ...
 Web-to-FW	Route table	West US	two-tier-resou... ...

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 address	West US	two-tier-resou... ...
 natPublicIP	Public IP address	West US	two-tier-resou... ...
.			

Custom Scripts/Linux Extensions

 db-vm-customscript	Microsoft.Com...	West US	two-tier-resou... ...
 nat-vm-customscript	Microsoft.Com...	West US	two-tier-resou... ...
 web-vm-customscript	Microsoft.Com...	West US	two-tier-resou... ...

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 and the nat-vm-customscript configures the NAT VM

4. Access the firewall

On successful deployment of template, the deployment summary will have an output section. The entire deployment takes about 24 minutes to complete.

The screenshot shows the Azure portal interface. On the left, there's a list of resources under 'Essentials' with a table showing items like 'db-vm-customscript', 'nat-vm-customscript', and 'web-vm-customscript'. On the right, the 'Deployment Summary' pane is open, showing details for three deployments:

- Microsoft.Template**: Deployment ID 0f3ba96c-a3c7-4eac-b599-ed9882801672, Status Succeeded, Duration 23 minutes 24 seconds, Resource Group two-tier-resource-group, Template Link <https://raw.githubusercontent.com/PaloAltoNetworks...>. This row has a red border around its content area.
- WeblinkedTemplate**: Deployment ID 1/30/2017, 5:01:10 PM, Status Succeeded.
- DBlinkedTemplate**: Deployment ID 1/30/2017, 5:00:58 PM, Status Succeeded.

Below the summary, there's an 'Outputs' section with two entries:

- VMSERIESURL: <https://pan-fwmij4.westus.cloudapp.azure.com>
- WEBSERVERURL: <http://pan-natmij4.westus.cloudapp.azure.com>

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

Palo Alto Networks Azure Resource Manager Template Deployment Guide

The screenshot shows the Palo Alto Networks PAN-OS 7.1 Dashboard. On the left, there's a sidebar with various icons for network components like Interfaces, Zones, Virtual Routers, and GlobalProtect. The main dashboard area has tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. A central window displays 'General Information' with details such as Device Name (pan-fw), MGT IP Address (10.5.0.4), and Model (PA-NM). To the right, there are several panels: 'Logged In Admins' (Admin panalto from 50.174.175.68), 'Config Logs' (No data available), 'Data Logs' (No data available), 'Locks' (No locks found), and 'ACC Risk Factor (Last 60 minutes)' (4.0). A large modal window titled 'Welcome to PAN-OS 7.1!' lists new features: SaaS Application Usage Report, Support for large-scale distributed User-ID deployment, Autofocus threat intelligence integration, Unified log view, Wildfire five-minute updates, External Dynamic Lists, Support for the VM-Series firewall in Microsoft Azure, Support for scaling the VM-Series firewall behind AWS Elastic Load Balancing (ELB), and Simplified deployment of two-factor authentication on GlobalProtect. Below the modal is a note about upgrading to the Content Release version and a checkbox for 'Do not show again'.

Here are the interfaces to zone mappings:

The screenshot shows the Palo Alto Networks PAN-OS 7.1 Network tab. On the left, there's a sidebar with icons for various network components. The main area has tabs for Ethernet, Loopback, and Tunnel. A table lists interface mappings:

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1	Layer3		Online	Dynamic-DHCP Client	default	Untagged	none	Untrust		
ethernet1/2	Layer3		Online	Dynamic-DHCP Client	default	Untagged	none	Trust		
ethernet1/3			Online	none	none	Untagged	none	none		
ethernet1/4			Online	none	none	Untagged	none	none		

In the policies tab, you can review the security policies:

Palo Alto Networks Azure Resource Manager Template Deployment Guide

Name	Tags	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action	Profile	Options
SSH inbound	none	universal	Untrust	any	any	any	Trust	any	ping	application-d...	Allow	none	
SSH 221-222 inbound	none	universal	Untrust	any	any	any	Trust	any	ping	ssh	service-tcp-2...	Allow	none
Allow all ping	none	universal	any	any	any	any	any	any	ping	application-d...	Allow	none	
Web browsing	none	universal	Untrust	any	any	any	Trust	any	ping	service-tcp-2...	Allow	none	
Allow all outbound	none	universal	Trust	any	any	any	Untrust	any	ping	application-d...	Allow	none	
Web to DB	none	universal	any	web-object	any	any	any	any	db-object	mysql	application-d...	Allow	
Log default deny	none	universal	any	any	any	any	any	any	any	any	application-d...	Deny	none
Intrazone-default	none	intrazone	any	any	any	(Intrazone)	any	any	any	any	allow	none	none
Interzone-default	none	interzone	any	any	any	any	any	any	any	any	deny	none	none

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.

There is also a rule for source NAT from web and db servers to the outside world.

Name	Tags	Original Packet						Translated Packet		
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	
Web SSH	none	Untrust	Untrust	any	any	service-tcp-2...	dynamic-ip-and-port	address: 10.5.3.5		
DB SSH	none	Untrust	Untrust	any	any	service-tcp-2...	dynamic-ip-and-port	port: 22		
WordPress NAT	none	Untrust	Untrust	any	any	service-http	dynamic-ip-and-port	address: 10.5.4.5		
Outbound nat	none	any	Untrust	any	any	any	dynamic-ip-and-port	port: 22		
							ethernet1/2	address: 10.5.3.5		
							ethernet1/2	port: 80		
							ethernet1/1	none		

5. Access the Webserver

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

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should [replace this file](#) (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

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

The screenshot shows the Palo Alto Networks Firewall interface. On the left, there's a navigation bar with 'Dashboard', 'ACC', 'Monitor' (which is selected), 'Policies', 'Objects', 'Network', and 'Device'. Below the navigation is a sidebar with icons for Log, Traffic, Threat, URL Filtering, Wildfire Submissions, Data Filtering, HPM Match, and Configuration. The main area is titled '(app eq web-browsing)' and contains a table of log entries. The columns are: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. There are three entries in the log table.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Action	Rule	Session End Reason	Bytes
01/30 23:22:57	end	Untrust	Trust	10.5.5.4		10.5.1.4	80	allow	Web browsing	tcp-fin	1.9k
01/30 23:22:56	end	Untrust	Trust	10.5.5.4		10.5.1.4	80	allow	Web browsing	tcp-fin	5.1k
01/30 23:22:56	end	Untrust	Trust	10.5.5.4		10.5.1.4	80	allow	Web browsing	tcp-fin	5.0k

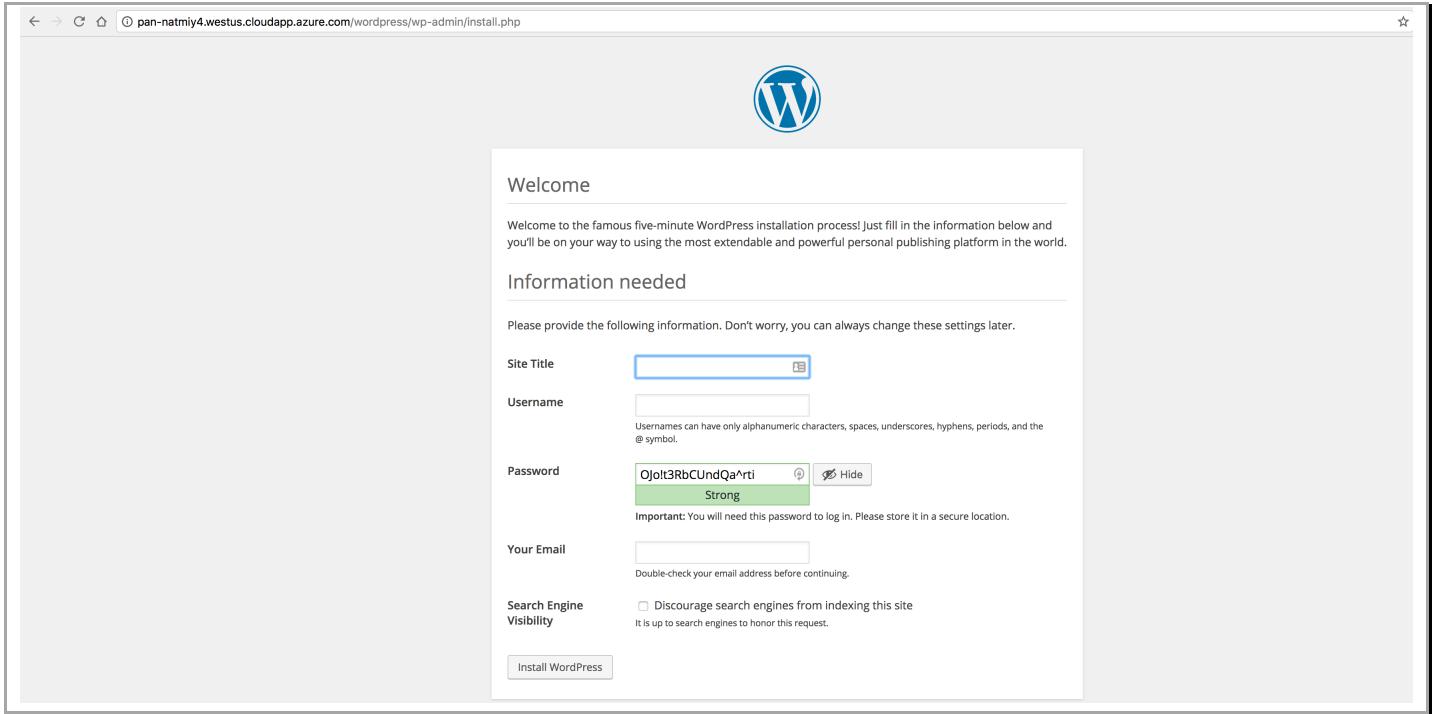
Now let us verify we pass east-West traffic through the firewall. In the browser, head to the wordpress server (<http://webserverURL/wordpress>) this should be the second link in the output section of the deployment tab

The screenshot shows the Azure Resource Manager Deployment blade. On the left, there's a 'Essentials' section with 'Subscription name (change) Narayan-pay-as-you-go', 'Subscription ID 0f3ba96c-a3c7-4eac-b599-ed9882801672', 'Deployments 3 Succeeded', and a 'Filter by name...' search bar. Below this is a table of resources with columns: NAME, TYPE, LOCATION, RESOURCE The resources listed are: db-vm-customscript (Microsoft.Compute VM), nat-vm-customscript (Microsoft.Compute VM), web-vm-customscript (Microsoft.Compute VM), DBeth0 (Network interface), FWeth0 (Network interface), and FWeth1 (Network interface). On the right, there's a 'Summary' section with deployment details: DEPLOYMENT DATE 1/30/2017, 5:01:16 PM, STATUS Succeeded, DURATION 23 minutes 24 seconds, RESOURCE GROUP two-tier-resource-group, RELATED Events, and TEMPLATE LINK <https://raw.githubusercontent.com/PaloAltoNetworks...>. At the bottom, there's a 'Outputs' section with two entries: VMSERIESURL with value <https://pan-fwmij4.westus.cloudapp.azure.com> and WEBSERVERURL with value <http://pan-natmij4.westus.cloudapp.azure.com>.

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.

Palo Alto Networks Azure Resource Manager Template Deployment Guide



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

A screenshot of the Palo Alto Networks Firewall interface. The left sidebar shows 'Logs' under 'Traffic'. The main pane displays a table of logs with the search term '(app eq mysql)'. The columns are: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. The table shows four entries related to MySQL traffic between the web server and database.

You have now successfully deployed an ARM template with a VM-Series firewall in Azure.

6. Launch some attacks

a. SSH from Web Server to DB Server

Let's 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**.

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:

The screenshot shows the Palo Alto Networks Firewall interface with the 'Monitor' tab selected. In the left sidebar, 'Logs' is expanded, showing 'Traffic', 'Threat', 'URL Filtering', 'WildFire Submissions', 'Data Filtering', 'HDP Match', 'Configuration System', 'Alarms', and 'Unified'. The main area displays a table titled '(port.dst eq 22)' with the following columns: Receive Time, Type, From Zone, To Zone, Source, Source User, Destination, To Port, Application, Action, Rule, Session End Reason, and Bytes. There are five rows of data, each representing a failed SSH attempt from source IP 10.5.3.5 to destination IP 10.5.4.5 on port 22. All entries show 'deny' as the action and 'Log default deny' as the rule.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
01/30 23:36:23	drop	Trust	Trust	10.5.3.5		10.5.4.5	22	not-applicable	deny	Log default deny	policy-deny	74
01/30 23:36:22	drop	Trust	Trust	10.5.3.5		10.5.4.5	22	not-applicable	deny	Log default deny	policy-deny	74
01/30 23:34:07	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54
01/30 23:20:13	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54
01/30 22:58:14	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54

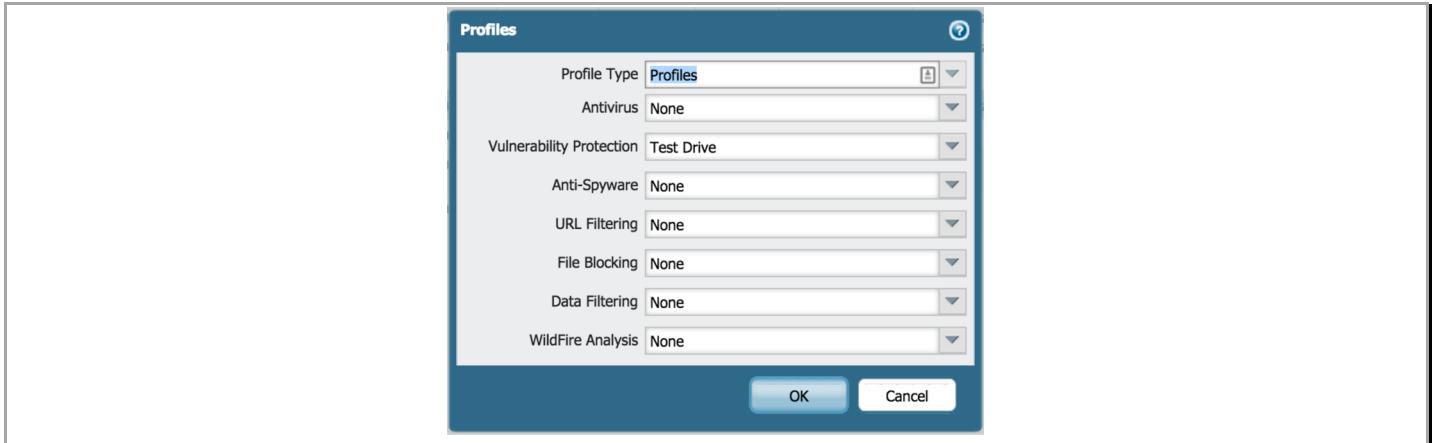
b. SQL Brute force attack

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:

The screenshot shows the Palo Alto Networks Firewall interface with the 'Policies' tab selected. In the left sidebar, 'Security' is expanded, showing 'NAT', 'QoS', 'Policy Based Forwarding', 'Decryption', 'Application Override', 'Captive Portal', and 'DoS Protection'. The main area displays a table with the following columns: Name, Tags, Type, Zone, Address, User, HIP Profile, Source, Destination, Application, Service, Action, Profile, and Options. There are nine rows of data, each representing a security rule. Rule 6, 'Web to DB', is highlighted in yellow. It has a 'universal' type, 'any' source and destination addresses, and 'any' user. The 'Profile' column for this rule shows a green icon, indicating it is protected by a threat protection profile.

Name	Tags	Type	Zone	Address	User	HIP Profile	Source	Destination	Application	Service	Action	Profile	Options
1 SSH inbound	none	universal		any	any	any		any					
2 SSH 221-222 inbound	none	universal		any	any	any		any					
3 Allow all ping	none	universal	any	any	any	any	any	any					
4 Web browsing	none	universal		any	any	any		any					
5 Allow all outbound	none	universal		any	any	any		any					
6 Web to DB	none	universal	any		any	any		any					
7 Log default deny	none	universal	any	any	any	any	any	any					
8 Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any					
9 Interzone-default	none	interzone	any	any	any	any	any	any					

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:

A screenshot of the Palo Alto Networks Firewall interface showing the "Monitor" tab selected. In the left sidebar, "Threat" is selected under "Logs". The main area displays a table of threat logs. One row is highlighted in yellow and shows the following details:

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	

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.

