

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.....	5
2.1 Create an Azure account	5
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	17
5. Access the Webserver.....	20
6. Launch some attacks.....	21
a. SSH from Web Server to DB Server	21
b. SQL Brute force attack	22
7. Cleanup	24

Version History

Version number	Comments
1.0	Initial GitHub check-in
1.1	Removed NAT instance

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:

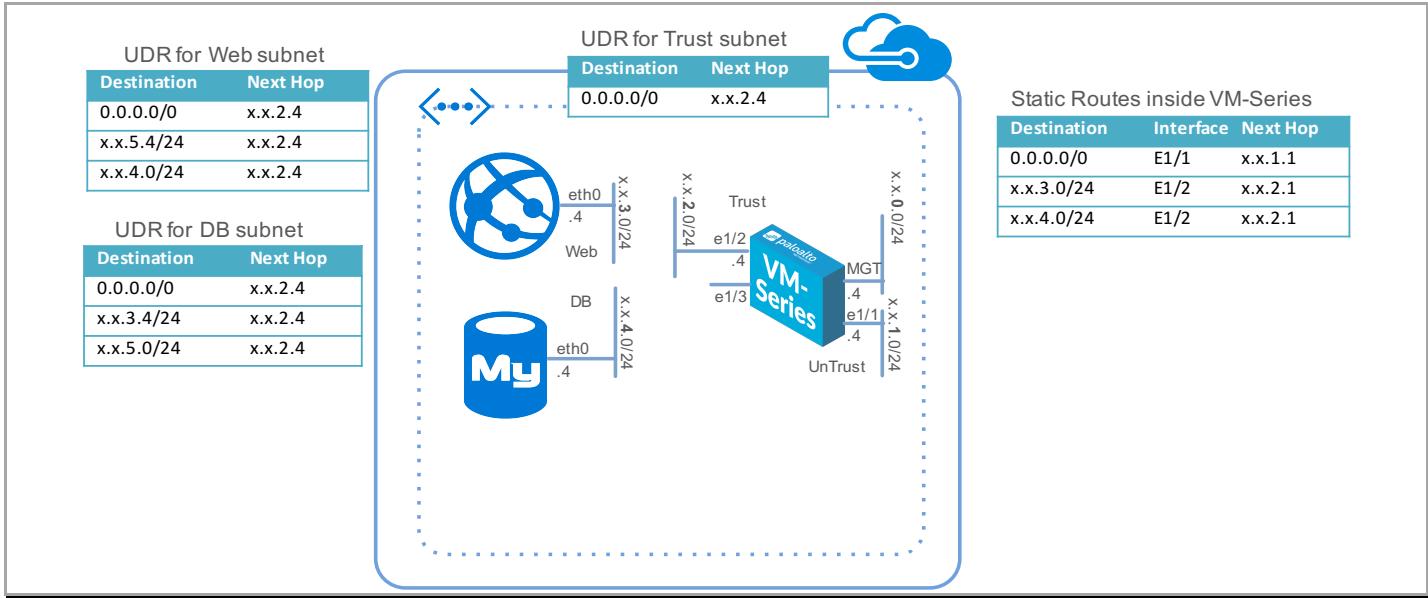
<https://azure.microsoft.com/en-us/documentation/templates/>

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>

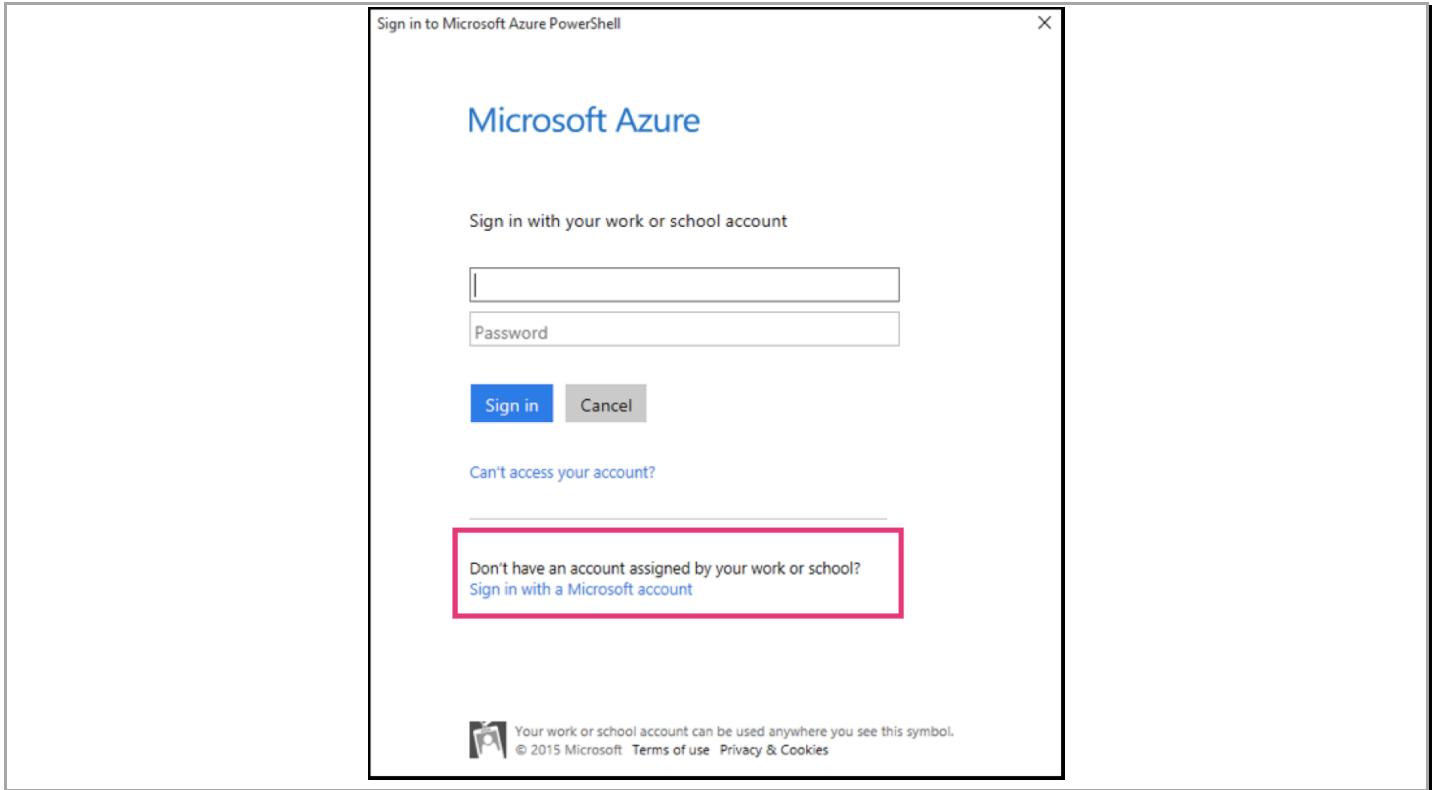
2. Prerequisites

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".



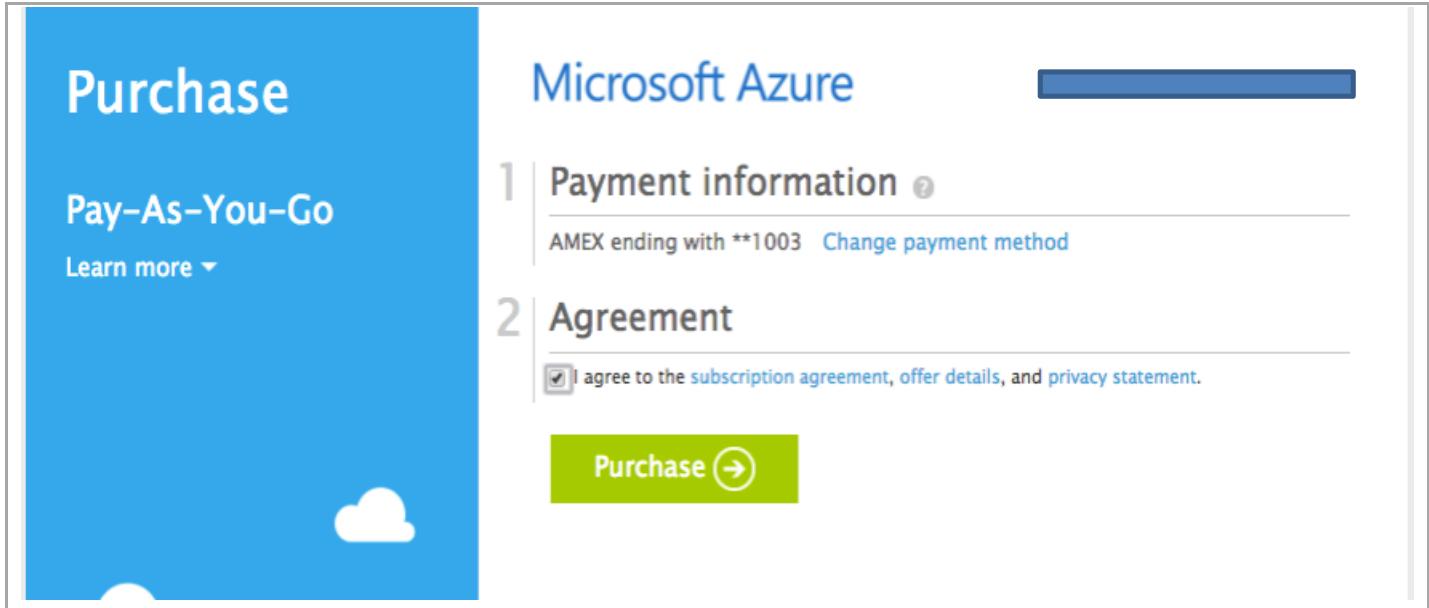
The free trial expires 30 days from account creation date or when \$200 free credits are used up.

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.

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.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

Microsoft Azure New > Custom deployment

Custom deployment

Deploy from a custom template

TEMPLATE

Customized template
20 resources

Edit **Learn more**

BASICS

* Subscription: **Create new** **Use existing**

* Resource group:

* 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 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	pay-as-you-go
* Resource group ⓘ	<input checked="" type="radio"/> Create new <input type="radio"/> Use existing two-tier-resource-grp
* 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 ⓘ	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 ⓘ	pan-fw
---------------------	--------

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

Web Server Dns Name ⓘ	pan-web
-----------------------	---------

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”

The screenshot shows the "TERMS AND CONDITIONS" section of the Azure Marketplace. It includes links to "Azure Marketplace Terms" and "Azure Marketplace". A detailed legal text describes the user's agreement to terms, authorizing Microsoft to charge and share contact information. Below the text is a checkbox labeled "I agree to the terms and conditions stated above" which is checked. There is also an unchecked option "Pin to dashboard". At the bottom is a large blue "Purchase" button.

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.

The screenshot shows the Microsoft Azure Resource Groups blade. On the left sidebar, "Resource groups" is selected and highlighted with a red box. In the main pane, a resource group named "two-tier-resource-grp" is selected and highlighted with a red box. On the right, the "Deployments" section is shown, indicating "1 Deploying". A red arrow points from the selected resource group in the center to the "Deployments" section on the right.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

Add Columns Delete Refresh Move

Essentials ^

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

Deployments
1 Deploying

Subscription ID [REDACTED]
Location West US

Filter by name...

18 items

NAME	TYPE	LOCATION	RESOURCE GROUP	...
database-vm	Virtual machine	West US	two-tier-resource-grp	...
DBeth0	Network interface	West US	two-tier-resource-grp	...
DB-to-FW	Route table	West US	two-tier-resource-grp	...
DefaultNSG	Network security group	West US	two-tier-resource-grp	...
FWeth0	Network interface	West US	two-tier-resource-grp	...
FWeth1	Network interface	West US	two-tier-resource-grp	...
FWeth2	Network interface	West US	two-tier-resource-grp	...
fwPublicIP	Public IP address	West US	two-tier-resource-grp	...
fwVNTEcz4	Virtual network	West US	two-tier-resource-grp	...
pan-fw	Virtual machine	West US	two-tier-resource-grp	...
storaecctecz4	Storage account	West US	two-tier-resource-grp	...
Trust-to-intranetwork	Route table	West US	two-tier-resource-grp	...
Webeth0	Network interface	West US	two-tier-resource-grp	...
WebPublicIP	Public IP address	West US	two-tier-resource-grp	...
webserver-vm	Virtual machine	West US	two-tier-resource-grp	...
Web-to-FW	Route table	West US	two-tier-resource-grp	...

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

Essentials ^

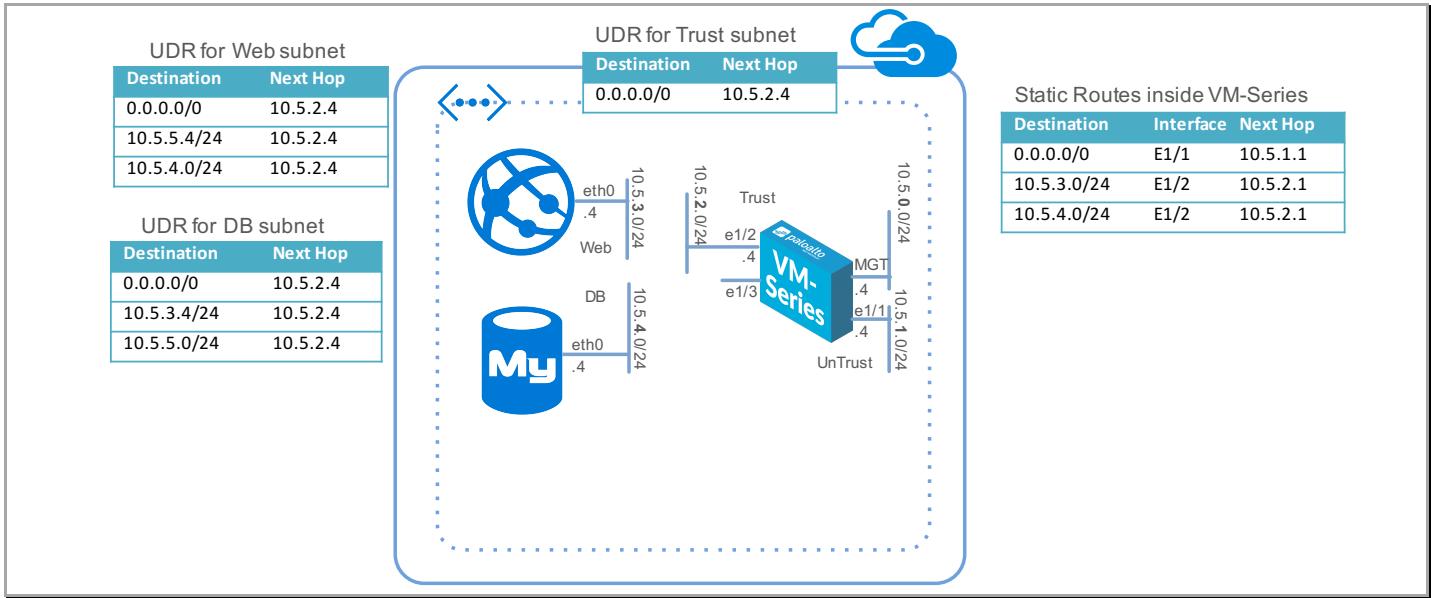
Subscription name (change)
[REDACTED] pay-as-you-go

Deployments
3 Succeeded

Subscription ID [REDACTED]
Location 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, 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.

 DBeth0	Network interface	West US
 FWeth0	Network interface	West US
 FWeth1	Network interface	West US
 FWeth2	Network interface	West US
 Webeth0	Network interface	West US

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	 pay-as-you... 
--	------------------	--------------------	---------	---

Palo Alto Networks Azure Resource Manager Template Deployment Guide

Inbound and outbound rules for the DefaultNSG

The screenshot displays two Azure portal windows side-by-side, both titled "DefaultNSG - [Rule Type] security rules".

Inbound security rules window:

- Left sidebar:** Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS, Inbound security rules (selected).
- Right pane:** A table titled "Search inbound security rules" with columns: PRIORITY, NAME, SOURCE, DESTINATI..., SERVICE, ACTION.
- Table Data:**

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

Outbound security rules window:

- Left sidebar:** Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS, Inbound security rules, Outbound security rules (selected).
- Right pane:** A table titled "Search outbound security rules" with columns: PRIORITY, NAME, SOURCE, DESTINATION, SERVICE, ACTION.
- Table Data:**

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
65000	AllowVnetOutBound	VirtualNetwork	VirtualNetwork	Custom (Any/Any)	Allow
65001	AllowInternetOutBound	Any	Internet	Custom (Any/Any)	Allow
65500	DenyAllOutBound	Any	Any	Custom (Any/Any)	Deny

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

4. Access the firewall

On successful deployment of template, the deployment summary will have an output section. The entire deployment takes about 10 minutes to complete.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

The screenshot shows the Azure portal's 'Deployments' blade. It lists three successful deployments:

- Microsoft.Template** (3/27/2017, 8:58:47 PM)
- WeblinkedTemplate** (3/27/2017, 8:58:42 PM)
- DBlinkedTemplate** (3/27/2017, 8:58:23 PM)

The 'Outputs' section displays two outputs:

- VMSeriesURL**: <https://pan-fwec4.westus.cloudapp.azure.com>
- WebServerURL**: <http://pan-webecz4.westus.cloudapp.azure.com>

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

The screenshot shows the PAN-OS 7.1 dashboard. The 'General Information' section includes the following details:

- Device Name: pan-fw
- MGT IP Address: 10.5.0.4 (DHCP)
- MGT Netmask: 255.255.255.0
- MGT Default Gateway: 10.5.0.1
- MGT IPv6 Address: unknown
- MGT IPv6 Link Local Address: fe80::20d:3aff:fe33:515b/64
- MGT IPv6 Default Gateway: 00:0c:3e:33:51:5b
- Model: PA-VH
- Serial #: A1E72961BD1527
- CPU ID: A2RPAVYv300nbnd2
- UUID: 1EF2961-BD15-274F-88B4-F5D9D2807988
- VM License: VM-300
- VM Mode: Microsoft Azure
- Software Version: 7.1.1
- GlobalProtect Agent: 0.0.0
- Application Version: 657-3825 (01/28/17)
- Threat Version: 657-3825 (01/28/17)
- URL Filtering Version: 20170130.40094
- Time: Mon Jan 30 23:08:10 2017
- Uptime: 0 days, 6:29:05

The 'System Resources' section shows:

- Management CPU: 2%
- Data Plane CPU: 0%
- Session Count: 2 / 249998

A modal window titled 'Welcome to PAN-OS 7.1!' lists new features:

- SaaS Application Usage Report for visibility into sanctioned and unsanctioned SaaS applications running on your network.
- Support for AWS Lambda, distributed low-to-no-deployment.
- Autofocus threat intelligence integration with PAN-OS logs.
- Unified log view showing all traffic and threat-related logs on a single page.
- Wildfire five-minute updates for detecting and blocking zero-day malware and exploits within minutes of discovery.
- External Dynamic Lists (formerly Dynamic Block List) extended to support URLs and custom domains.
- Support for the VM-Series Firewall in Microsoft Azure.
- Support for scaling the VM-Series Firewall behind AWS Elastic Load Balancing (ELB).
- Simplified deployment of two-factor authentication on GlobalProtect.

At the bottom of the modal, it says: "For a complete description of the new features and instructions on how to use them, refer to the PAN-OS 7.1 New Features Guide. To ensure that you can take advantage of all of the new features, you must upgrade the Content Release version. Refer to the PAN-OS 7.1 Release Notes for the content version required."

Here are the interfaces to zone mappings:

Palo Alto Networks Azure Resource Manager Template Deployment Guide

The screenshot shows the Palo Alto Networks UI with the Network tab selected. On the left, there's a sidebar with various icons for security features like IPsec, DHCP, DNS, and GlobalProtect. The main area has tabs for Ethernet, Loopback, and Tunnel, with Ethernet selected. A table lists four interfaces: ethernet1/1, ethernet1/2, ethernet1/3, and ethernet1/4. Each interface is a Layer3 type, managed by Dynamic-DHCP Client, and has a default link state. They are all untagged and belong to the Untrust security zone.

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

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

The screenshot shows the Policies tab with a table of security rules. The columns include Name, Tags, Type, Zone, Address, User, HTTP Profile, Destination, Application, Service, Action, Profile, and Options. The rules allow SSH access (inbound and outbound), ping, web traffic (HTTP and MySQL), and database access (db-object). Some rules are deny actions.

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

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.

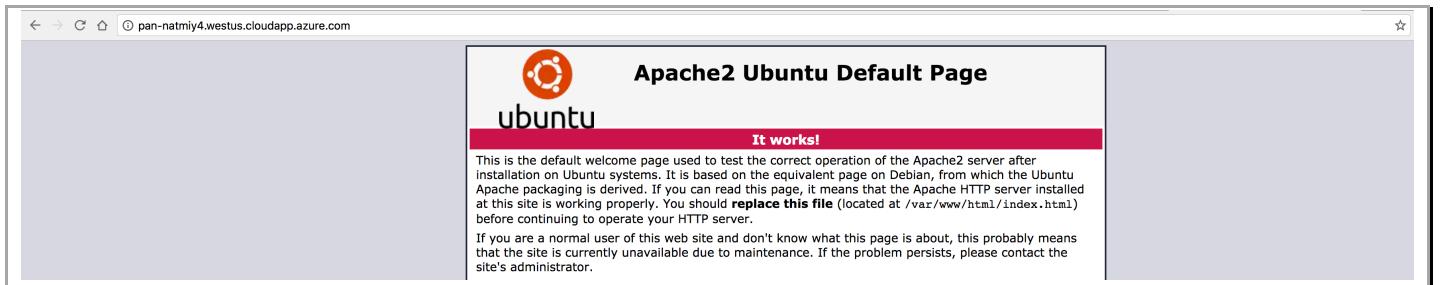
There is also a rule for source NAT from web and db servers to the outside world.

The screenshot shows the Policies tab with a table of NAT rules. The columns include Name, Tags, Source Zone, Destination Zone, Destination Interface, Source Address, Destination Address, Service, Source Translation, and Destination Translation. The rules map traffic from internal interfaces (10.5.1.4, 10.5.1.1) to external addresses (10.5.3.5, 10.5.4.5) via dynamic-to-and-port translation.

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	10.5.1.4	service-tcp-...	dynamic-to-and-port ethernet1/2	
DB SSH	none	Untrust	Untrust	any	any	10.5.1.4	service-tcp-...	dynamic-to-and-port ethernet1/2	
WordPress NAT	none	Untrust	Untrust	any	any	10.5.1.4	service-http	dynamic-to-and-port ethernet1/2	
Outbound nat	none	any	Untrust	any	any	any	any	dynamic-to-and-port ethernet1/1	

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:



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

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

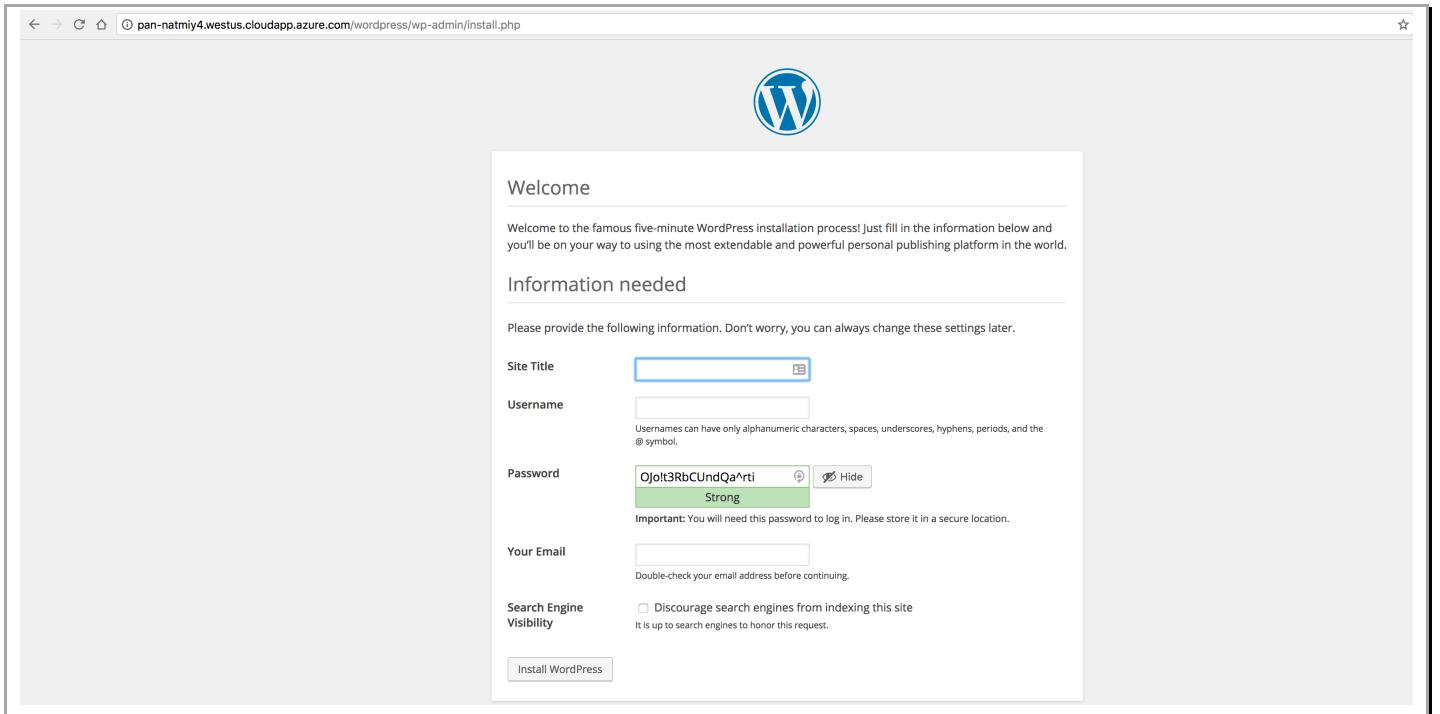
Now let us verify we pass east-West traffic through the firewall. In the browser, head to the wordpress server (<http://webserverURL/wordpress>) this should be the second link in the output section of the deployment tab

NAME	TYPE	VALUE
VMSERIESURL	String	https://pan-fwecz4.westus.cloudapp.azure.com
WEBSERVERURL	String	http://pan-webecz4.westus.cloudapp.azure.com

And you should see the WordPress welcome page.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

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:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
01/30 23:26:59	end	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	allow	Web to DB	tcp-fin	20.7k
01/30 23:26:58	end	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	allow	Web to DB	tcp-fin	5.1k
01/30 23:26:44	start	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	allow	Web to DB	n/a	375
01/30 23:26:44	start	Trust	Trust	10.5.3.5		10.5.4.5	3306	mysql	allow	Web to DB	n/a	375

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.

Palo Alto Networks Azure Resource Manager Template Deployment Guide

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's monitor log table. The logs are filtered for port 22. There are four entries, all of which were dropped (denied) because they did not match any applicable rules. The details are as follows:

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 22:55:14	drop	Untrust	Untrust	10.5.5.4		10.5.1.4	22	not-applicable	deny	Log default deny	policy-deny	54

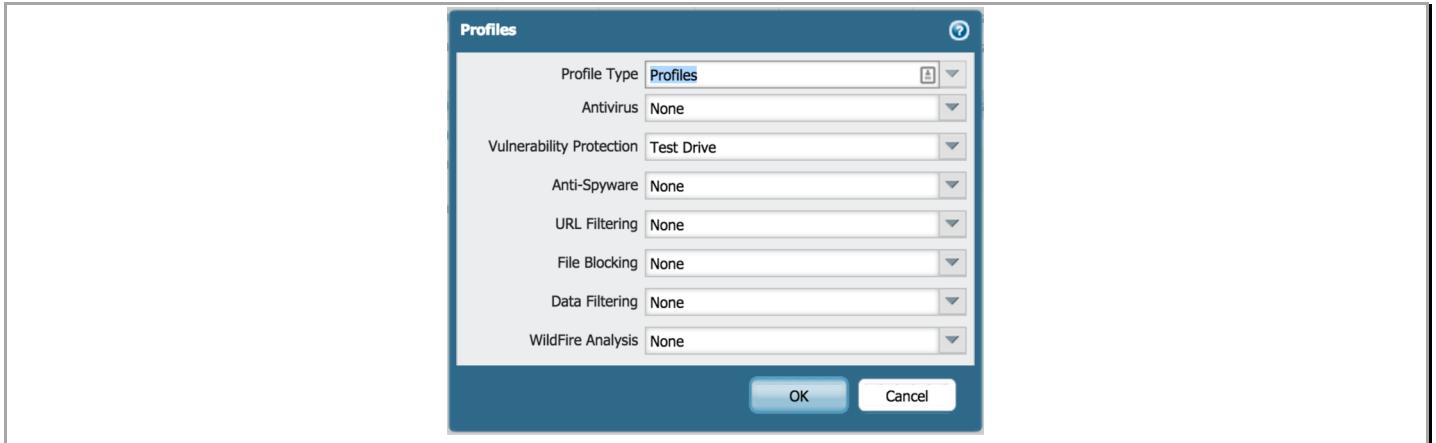
b. SQL Brute force attack

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's security policies table. Rule 6 is highlighted. It defines a source object (web-object) and a destination object (db-object). The destination is MySQL (mysql). The action is Allow, and the profile is application-d... (indicated by a shield icon). The policy also includes a service (mysql) and application (application-d...).

Name	Tags	Type	Zone	Address	User	HIP 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	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	service-tcp-...	Allow	none		
Allow all outbound	none	universal	Trust	any	any	any	Untrust	any	service-tcp-...	Allow	none		
Web to DB	none	universal	any	web-object	any	any	any	db-object	mysql	application-d...	Allow	shield	
Log default deny	none	universal	any	any	any	any	any	any	any	Deny	Deny	none	
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	Allow	Allow	none	
interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	Deny	none	

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.

