



05/17/2018

Two Firewalls in Load Balance Sandwich - DEMO

PALO ALTO NETWORKS

MATTHEW MCLIMANS

SYSTEMS ENGINEER

mmclimans@paloaltonetworks.com

Table of Contents

Network Diagram 2

Network Diagram: Inbound Request 3

Network Diagram: Outbound Request 4

Step 1. Deploy environment from GitHub 5

Step 2. Enter parameters for deployment 6

Step 3. Verify the deployment completed 7

Step 4. Login to the firewalls 8

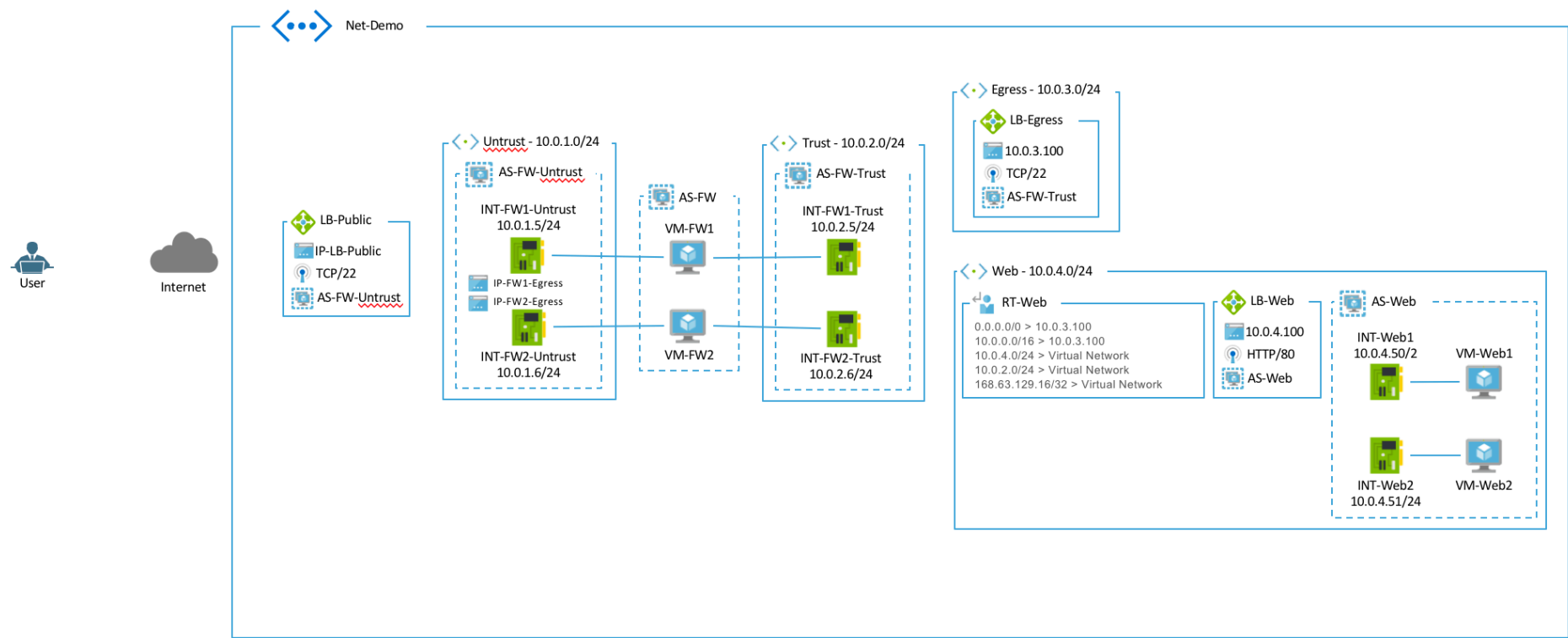
Step 5. Import and load the firewall configurations 9

Step 6. Test & view inbound SSH to web servers 10

Step 7. Test & view outbound connectivity 11

Network Diagram

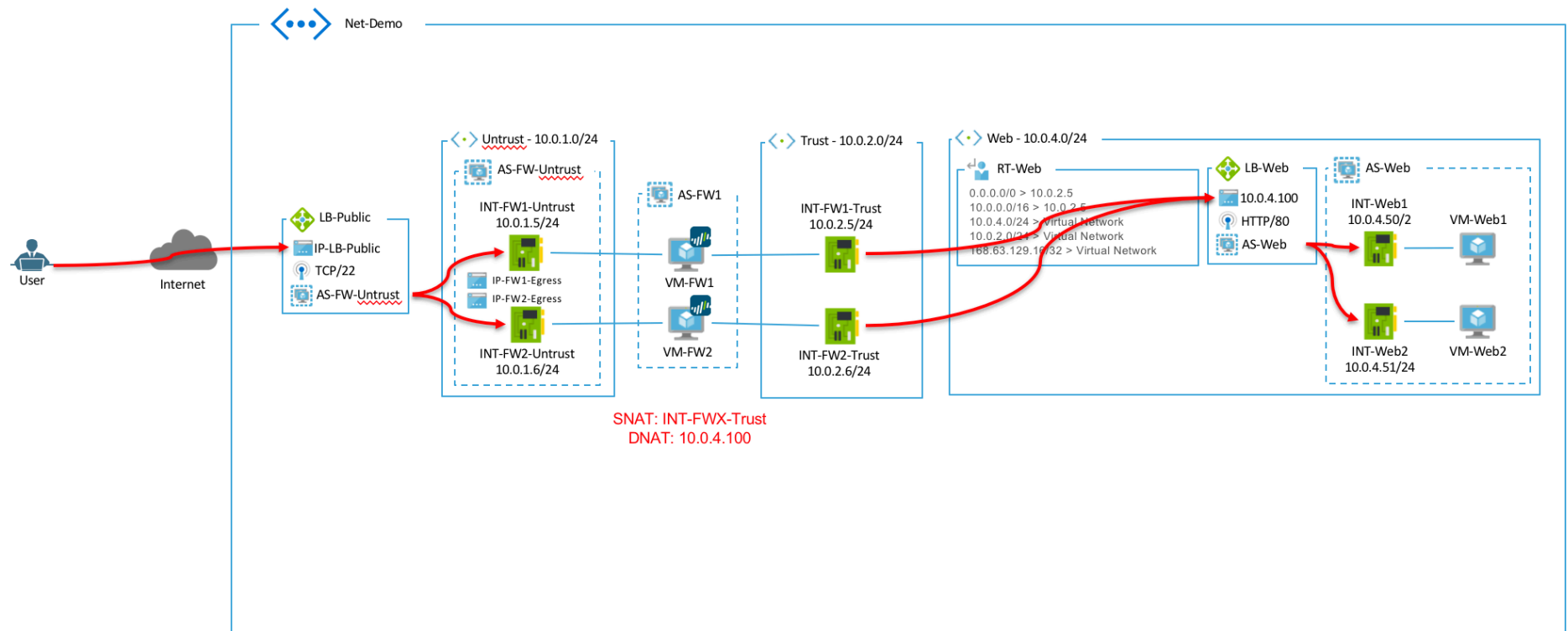
The diagram below illustrates the cloud components deployed from the GitHub template.



Network Diagram: Inbound Request

The diagram below illustrates an inbound request (i.e. HTTP, SSH) to a web-server.

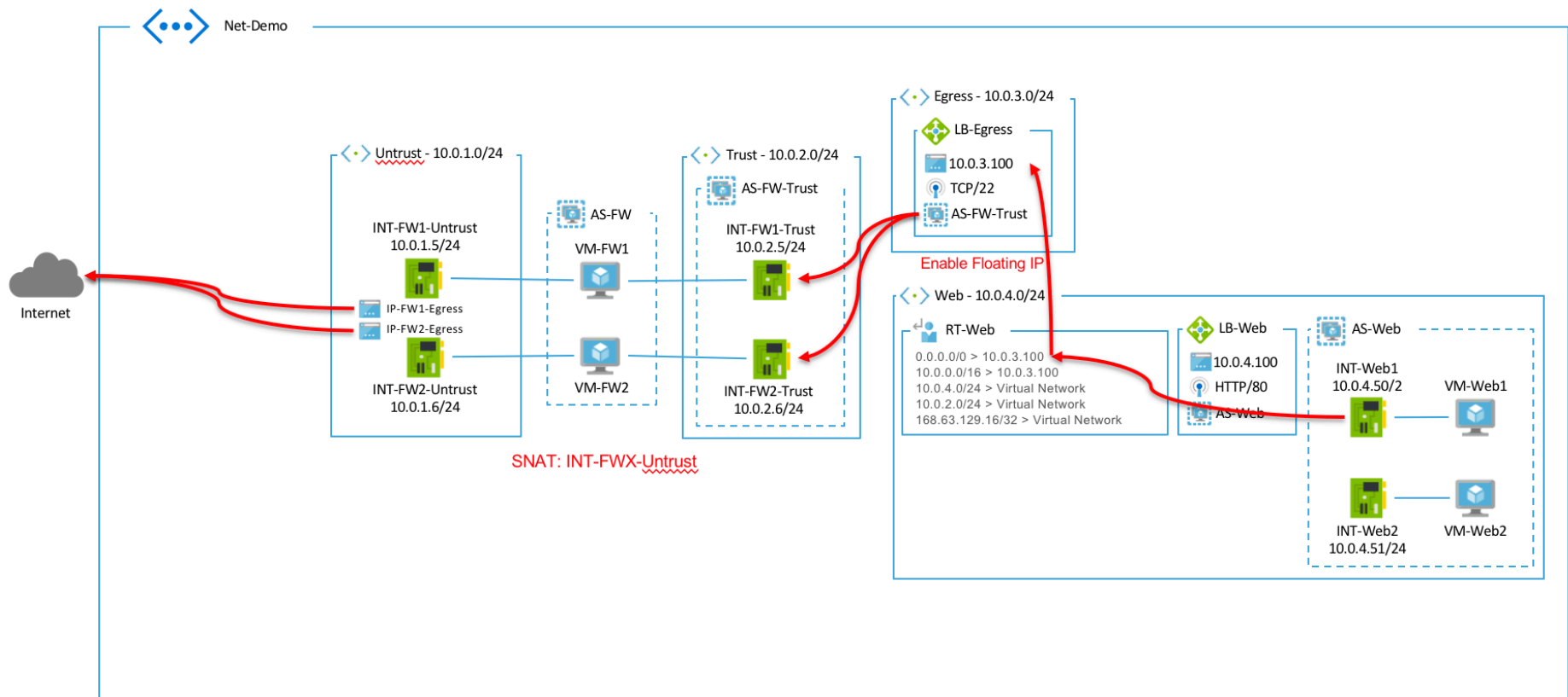
Inbound Request



Network Diagram: Outbound Request

The diagram below illustrates an outbound request (i.e. Ping, HTTP, HTTPS) to the internet.

Outbound Request



Step 1. Deploy environment from GitHub

(<https://github.com/mattmclimans/PaloAltoNetworks/tree/master/azure/demo/lb-sandwich>)

mattmclimans / PaloAltoNetworks

Watch 0

Star 0

Fork 0

<> Code

Issues 0

Pull requests 0

Projects 0

Wiki

Insights

Settings

Branch: master ▾

PaloAltoNetworks / azure / demo /

Create new file

Upload files

Find file

History

mattmclimans

Update azureDeploy.json

Latest commit b878ee6 22 minutes ago

..

README.md

Update README.md

2 hours ago

azureDeploy.json

Update azureDeploy.json

22 minutes ago

config-fw1

Add files via upload

an hour ago

config-fw2

Add files via upload

an hour ago

README.md

Deploy Palo Alto Networks Firewalls - Demo

Deploy to Azure

Step 2. Enter parameters for deployment


1. Create a new resource group. The resource group name must be unique to your environment.
2. Select License Type ([more info](#))
 - a. BYOL: Requires a license (evaluation licenses can be provided by Palo Alto Networks).
 - b. Bundle 1: Includes the VM-Series capacity license (VM-300 only), Threat Prevention license that includes IPS, AV, malware prevention, and a premium support entitlement.
 - c. Bundle 2: Includes the VM-Series capacity license (VM-300 only), Threat Prevention (includes IPS, AV, malware prevention), GlobalProtect, WildFire, PAN-DB URL Filtering licenses, and a premium support entitlement.
 - d.
3. Enter username and password
 - a. **RECORD USERNAME AND PASSWORD. THEY WILL BE NEEDED LATER.**

[Home](#) > Custom deployment

Custom deployment

Deploy from a custom template

TEMPLATE

 Customized template
25 resources

[Edit template](#)[Edit parameters](#)[Learn more](#)

BASICS

* Subscription

Visual Studio Professional

* Resource group

☒ Create new ☐ Use existing

my-resource-group

* Location

East US

SETTINGS

* Vm Size ⓘ

Standard_DS3_v2

* License Type ⓘ

bundle2

Username

paloalto

* Password

.....

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](#)

Step 3. Verify the deployment completed

- In the Azure portal, you can view the deployment process by clicking the Bell icon and clicking Deployment in progress...

The screenshot shows the Azure portal interface. The main pane displays the 'Microsoft.Template - Overview' page, which is in the 'Deploying' state. The deployment details are as follows:

Property	Value
Deployment name	Microsoft.Template
Status	Deploying
Subscription	Visual Studio Professional
Resource group	my-resource-group
Last modified	5/16/2018, 11:33:34 PM
Duration	2 minutes 35 seconds
Correlation ID	044c734c-a022-49f7-8dc9-27e7bcf6f8af

Below the details is a table of resources:

RESOURCE	TYPE	STATUS	TIMESTAMP
VM-FW1	Microsoft.Compute/virtualMachines	Created	5/16/2018, 11:34
VM-FW2	Microsoft.Compute/virtualMachines	Created	5/16/2018, 11:34
VM-Web2	Microsoft.Compute/virtualMachines	Created	5/16/2018, 11:34
VM-Web1	Microsoft.Compute/virtualMachines	Created	5/16/2018, 11:34
INT-Web2	Microsoft.Network/networkInterfaces	Created	5/16/2018, 11:33

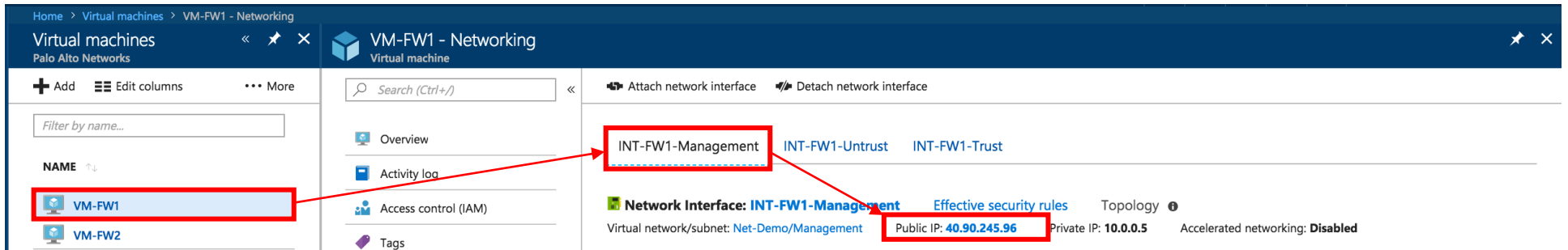
On the right, a 'Notifications' pane is open, showing a notification titled 'Deployment in progress...' with a 'Running' status. The notification text states: 'Deployment to resource group 'my-resource-group' is in progress.'

- Once the deployment has completed successfully, the following notification will appear in the Azure portal.

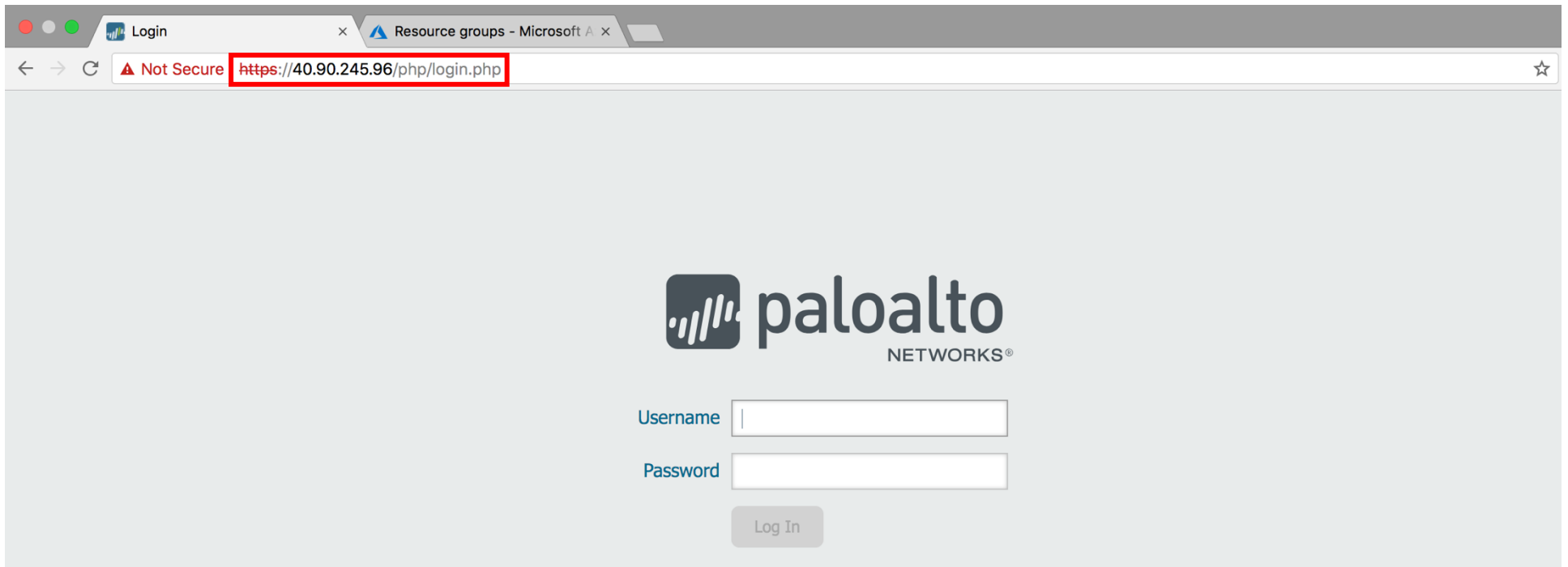
The screenshot shows the Azure portal interface with a 'Notifications' pane open. The notification is titled 'Deployment succeeded' and includes a green checkmark icon. The text of the notification is: 'Deployment 'Microsoft.Template' to resource group 'mrm-resource' was successful.' The notification is timestamped '12:32 PM'. At the bottom of the notification, there are two buttons: 'Go to resource group' and 'Pin to dashboard'.

Step 4. Login to the firewalls

1. In the Azure Portal go to: Virtual Machines→VM-FW1→Networking.
2. Click INT-FW1-Management to view the VM-FW1's management NIC settings.
3. Copy the public IP address listed (40.xxx.xxx.xxx). This is the public IP address for the firewall's management interface.

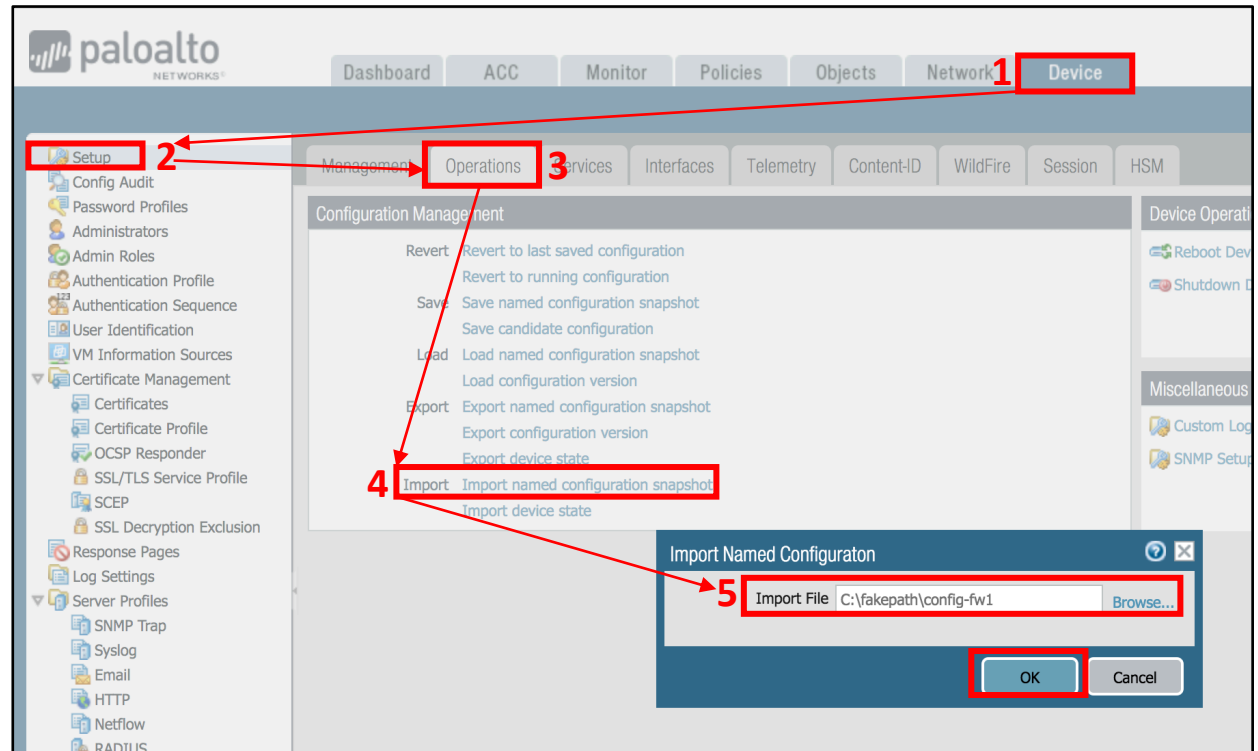


4. Open a new browser tab and paste the IP preceded by <https://> (i.e. <https://40.90.245.96>)
5. Repeat steps above for VM-FW2

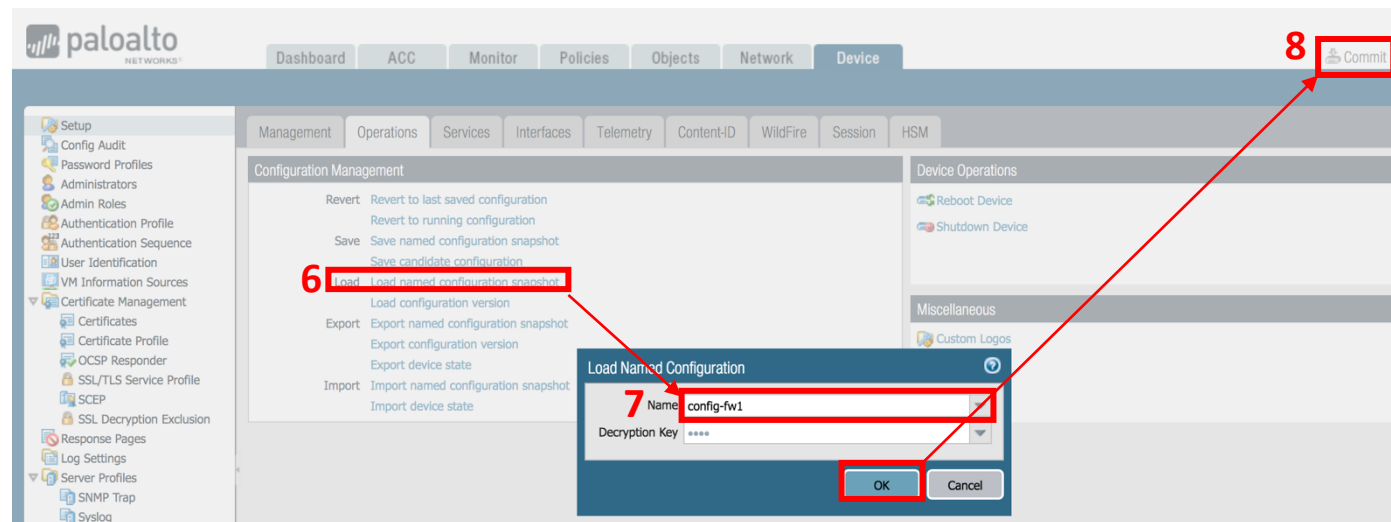


Step 5. Import and load the firewall configurations

1. Download config-fw1 and config-fw2 from the GitHub page.
2. On VM-FW1, go to: Device Tab → Setup → Import named configuration snapshot
3. Click Browse and select config-fw1 from your computer. Click Ok to import.



4. Click Load configuration snapshot and select config-fw1
5. Click Commit to apply changes
6. Repeat for VM-FW2 using the config-fw2 configuration file.



Step 6. Test & view inbound SSH to web servers

1. In the Azure Portal, go to Load Balancers → LB-Public → Front End Address
2. Copy the front-end IP address.

The screenshot shows the Azure Portal interface for the 'LB-Public' load balancer. The 'Overview' tab is selected, and the 'Public IP address' is highlighted as 40.90.240.161 (IP-LB-Public). The 'Essentials' section on the right shows the configuration details, including the resource group 'my-resource-group', location 'East US', and subscription ID '36a6952c-125c-4b32-943e-27e85b91d591'.

3. Using PuTTY (or equivalent), launch an SSH session using your username and password from Step 2. Use the Front-End IP address from LB-Public as the host address.
4. Once connected, on the firewalls go to Monitor Tab → Traffic to view the SSH session.

The screenshot shows the Palo Alto Networks firewall Monitor tab. The 'Traffic' tab is selected, and the logs show two successful SSH sessions. The first session is from 104.226.19.163 to 10.0.1.5 on port 22, and the second session is from 187.118.23.248 to 10.0.1.5 on port 22. Both sessions are allowed by the 'Allow All Inbound' rule.

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	05/16 20:51:47	end	Untrust	Trust	104.226.19.163		10.0.1.5	22	ssh	allow	Allow All Inbound	tcp-fin	3.6k
	05/16 20:49:37	end	Untrust	Trust	187.118.23.248		10.0.1.5	22	ssh	allow	Allow All Inbound	tcp-fin	1.8k

Inbound Final Result

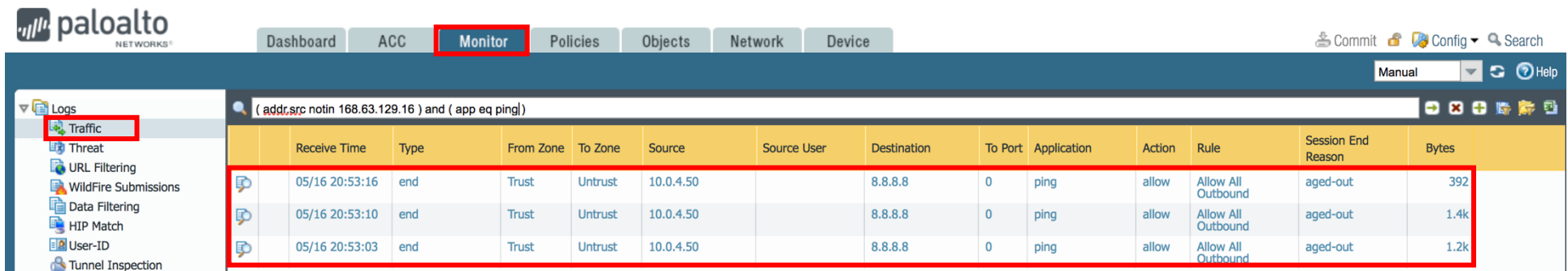
You will see that the SSH session completes to one of the web-servers (10.0.4.50 or 10.0.4.51). The SSH session traverses the Public Load Balancer (LB-Public). The public load balancer sends the session to one of the firewalls. Lastly, the firewall will forward the session to the web-servers load balancer frontend IP (LB-Web, 10.0.4.100). This is performed by the NAT policies on the firewall (Policies Tab → NAT).

Step 7. Test & view outbound connectivity

1. From the Linux server, try pinging out to the internet (i.e. ping 8.8.8.8). You can also ping laterally to the second web-server (10.0.4.50 or 10.0.4.51) . You can also try updating the Linux server (sudo apt-get update) to see additional traffic.

```
palocalto@VM-Web1: ~  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$  
palocalto@VM-Web1:~$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=3.23 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=3.10 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=2.85 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=2.85 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=2.83 ms  
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=3.21 ms  
64 bytes from 8.8.8.8: icmp_seq=7 ttl=53 time=3.62 ms  
64 bytes from 8.8.8.8: icmp_seq=8 ttl=53 time=3.52 ms
```

2. On the firewalls, go to Monitor Tab → Traffic to view the traffic.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	05/16 20:53:16	end	Trust	Untrust	10.0.4.50		8.8.8.8	0	ping	allow	Allow All Outbound	aged-out	392
	05/16 20:53:10	end	Trust	Untrust	10.0.4.50		8.8.8.8	0	ping	allow	Allow All Outbound	aged-out	1.4k
	05/16 20:53:03	end	Trust	Untrust	10.0.4.50		8.8.8.8	0	ping	allow	Allow All Outbound	aged-out	1.2k

Outbound Final Result

You will see that the outbound pings go through the firewalls. The ping from the Linux server goes through the internal load balancer (LB-Egress). This traffic is load balanced to one of the firewalls. Once the firewall receives the traffic, it is forwarded out through its untrust NIC to the internet. The return path takes the same path back.