05/17/2018

Two Firewalls in Load Balance Sandwich - DEMO

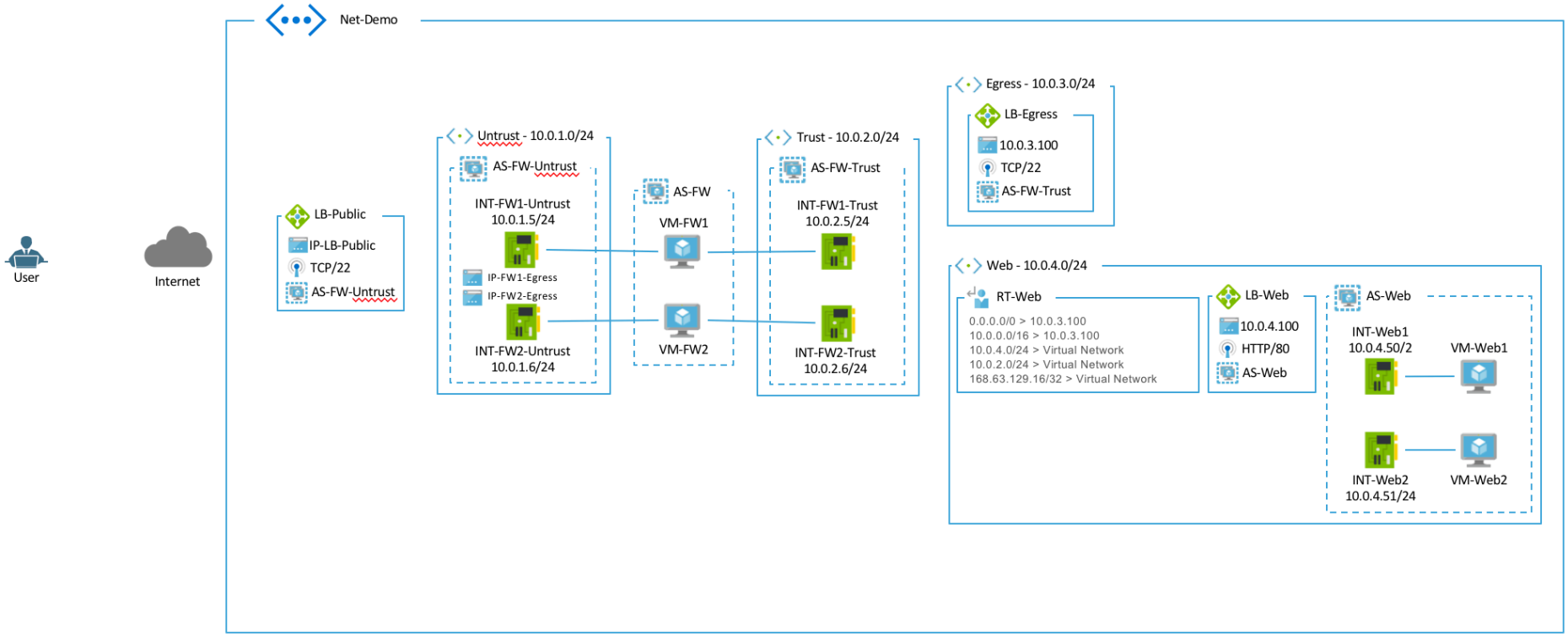
PALO ALTO NETWORKS

MATTHEW MCLIMANS
SYSTEMS ENGINEER
mmclimans@paloaltonetworks.com

Table of Contents

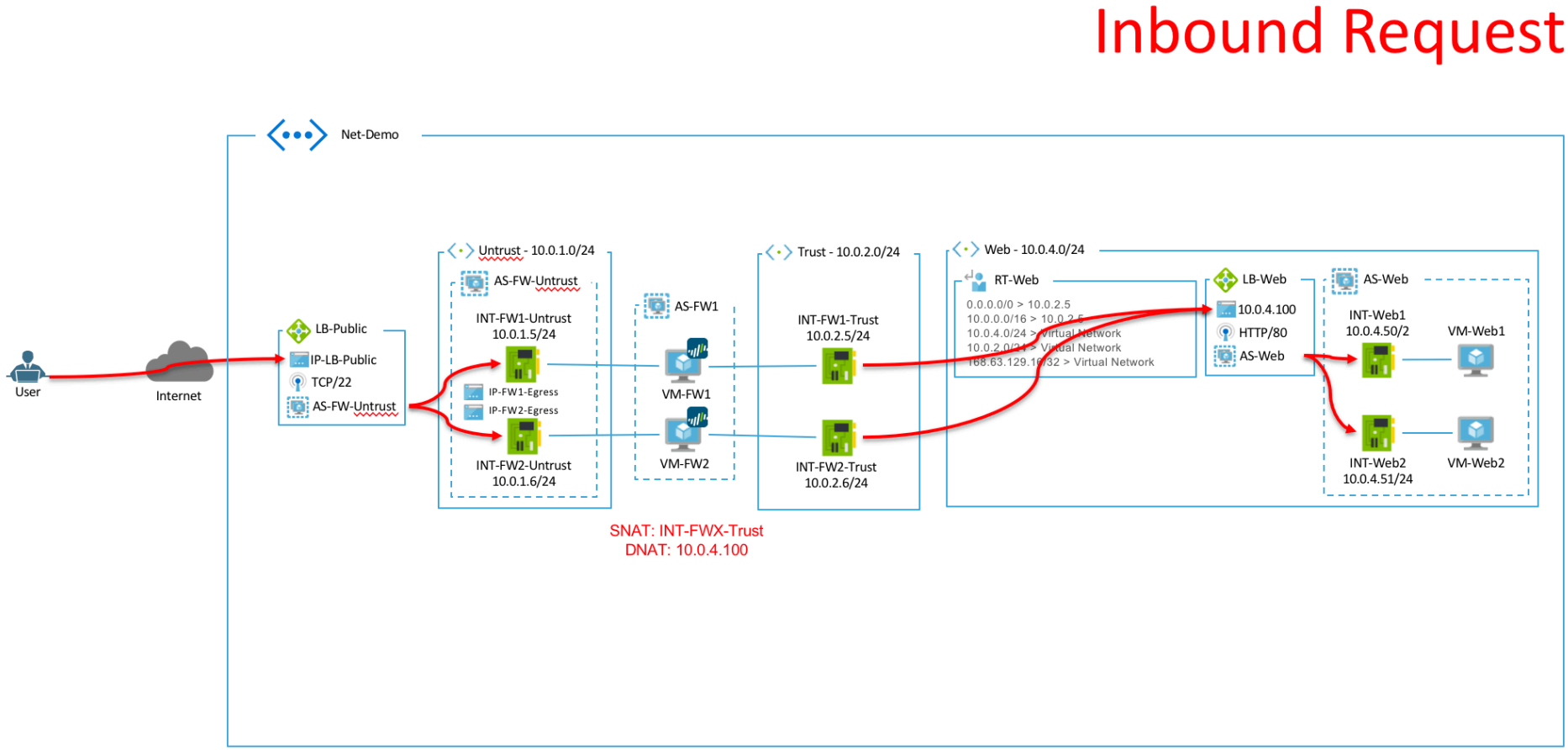
Network Diagram

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



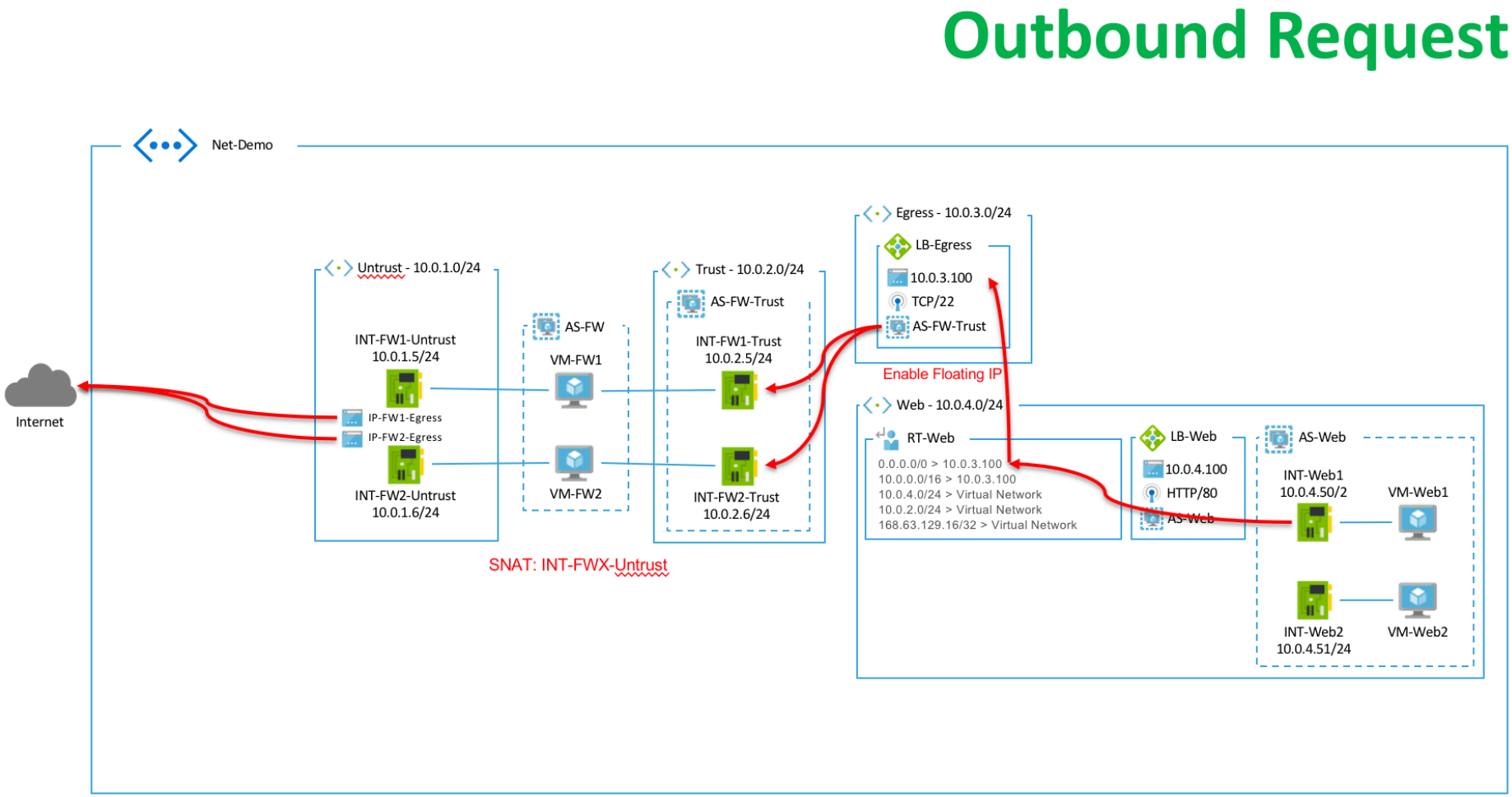
Network Diagram: Inbound Request

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



Network Diagram: Outbound Request

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



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

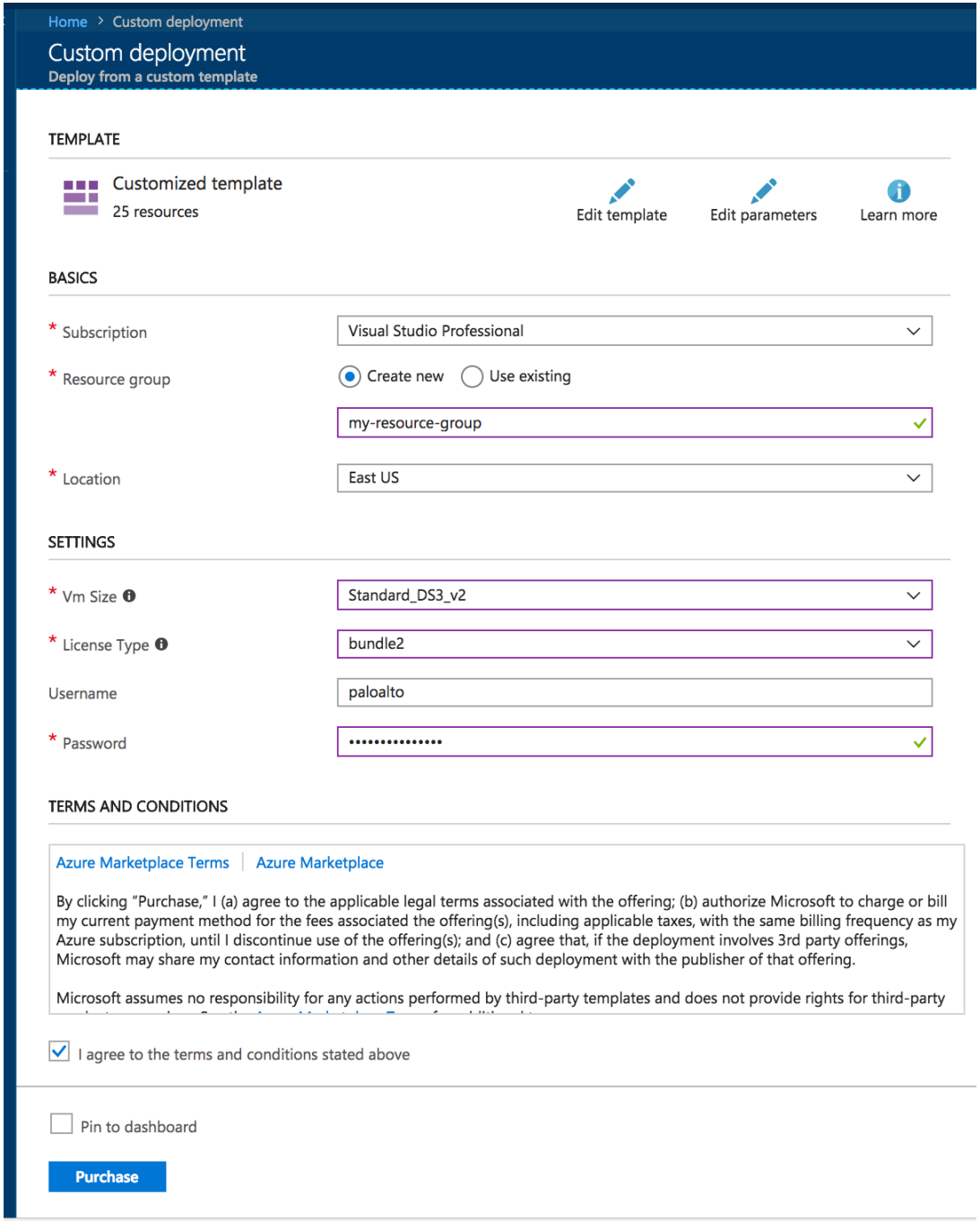
README.md

Deploy Palo Alto Networks Firewalls - Demo

Deploy to Azure

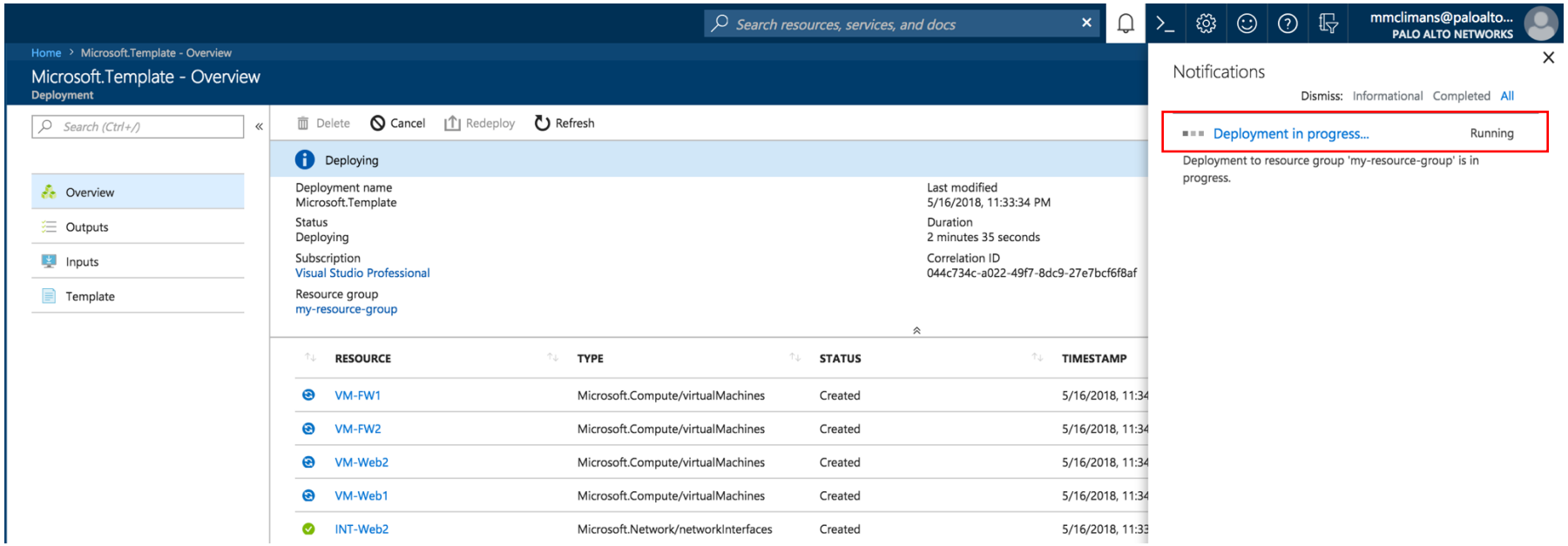
Step 2. Enter parameters for deployment

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.

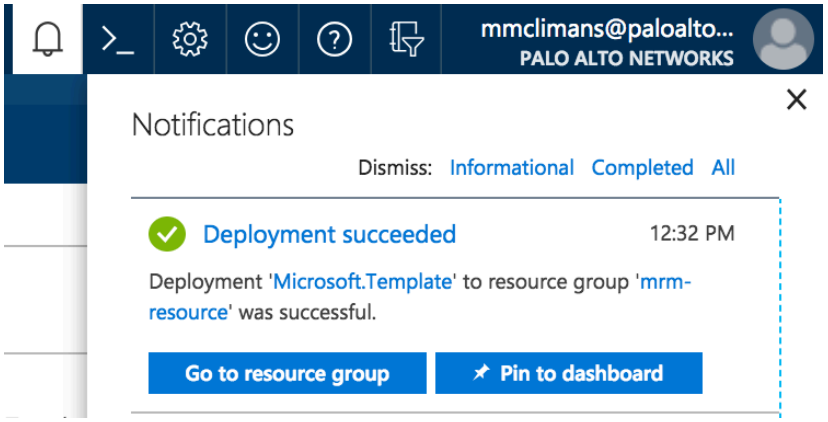


Step 3. Verify the deployment completed

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

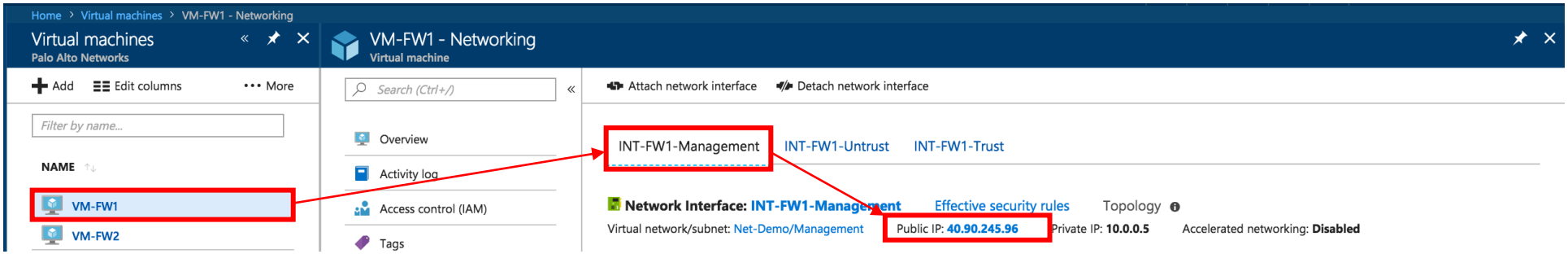


- Once the deployment has completed successfully, the following notification will appear in the Azure portal.

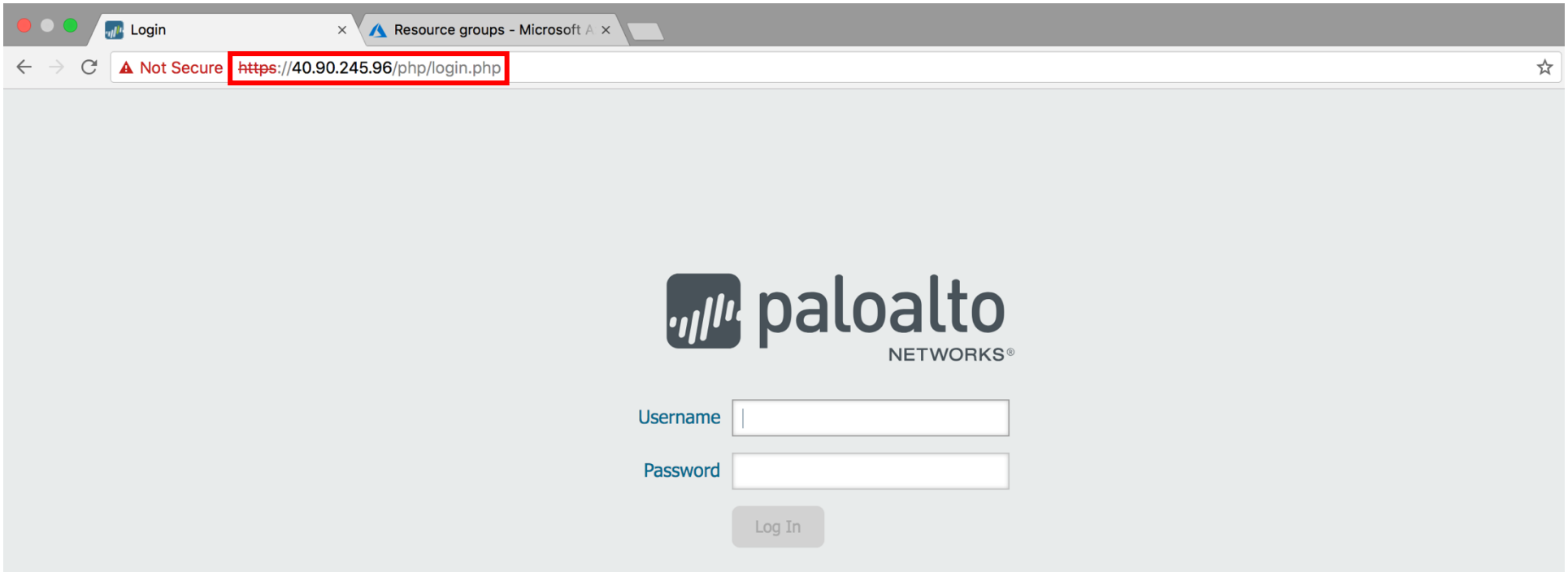


Step 4. Login to the firewalls

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.

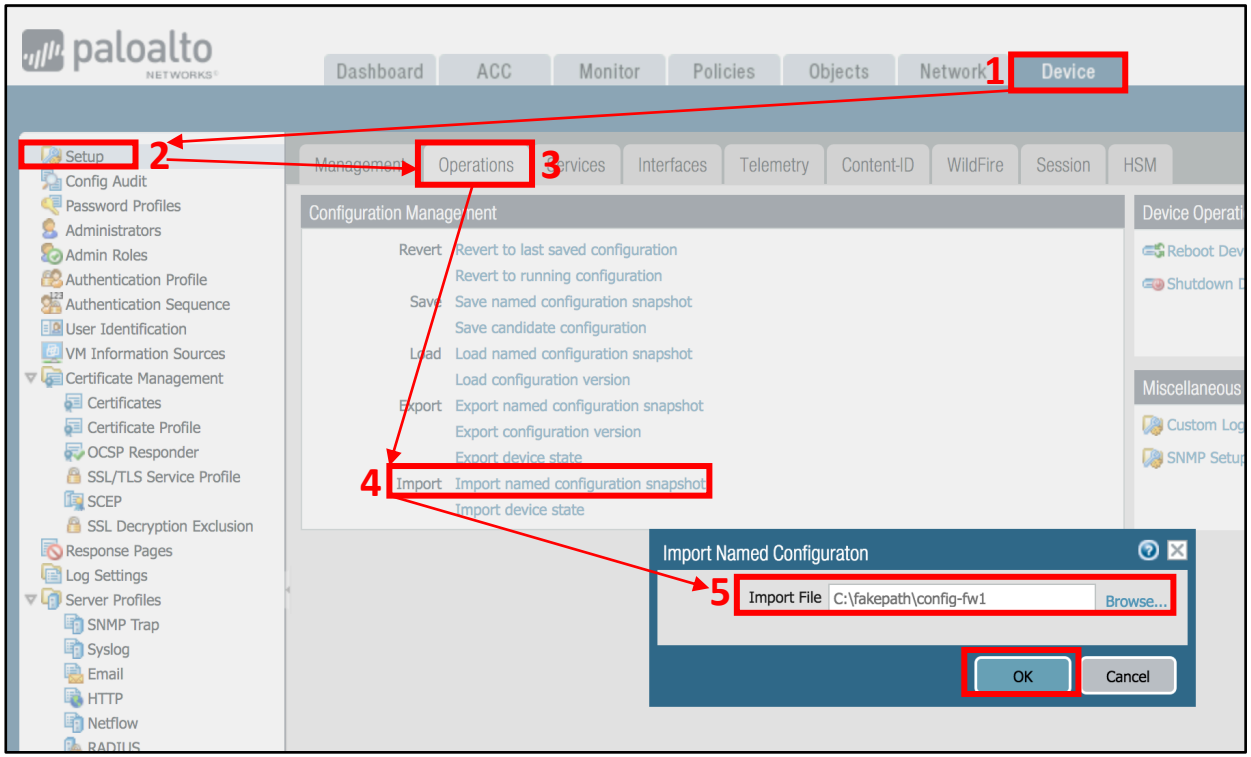


4. Open a new browser tab and paste the IP preceded by https:// (i.e. https://40.90.245.96)
5. Repeat steps above for VM-FW2

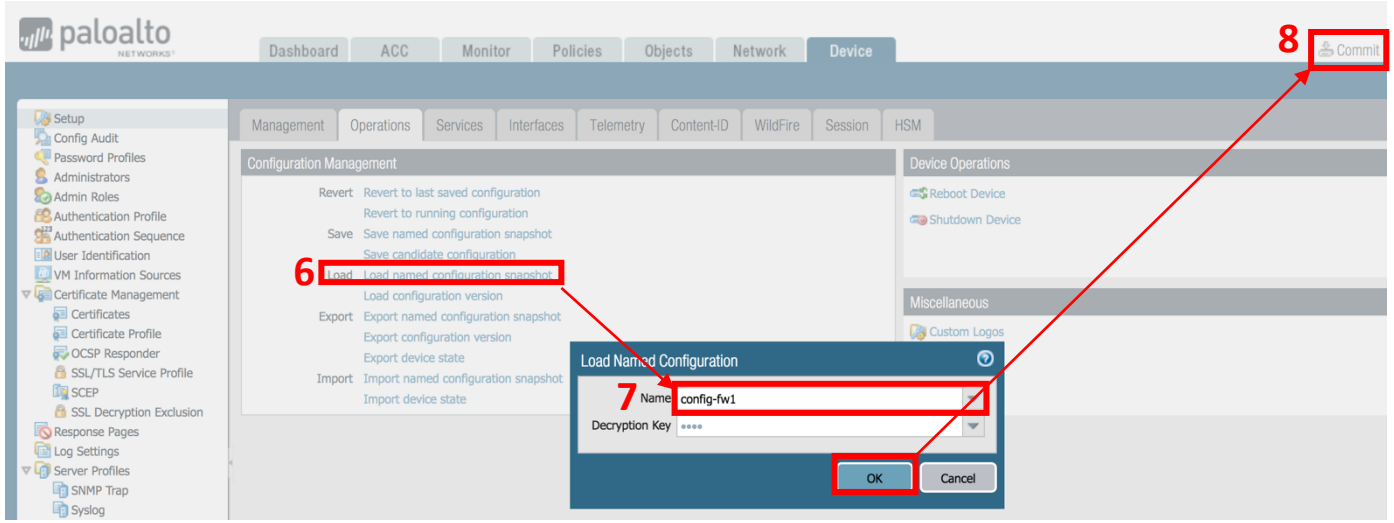


Step 5. Import and load the firewall configurations

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.

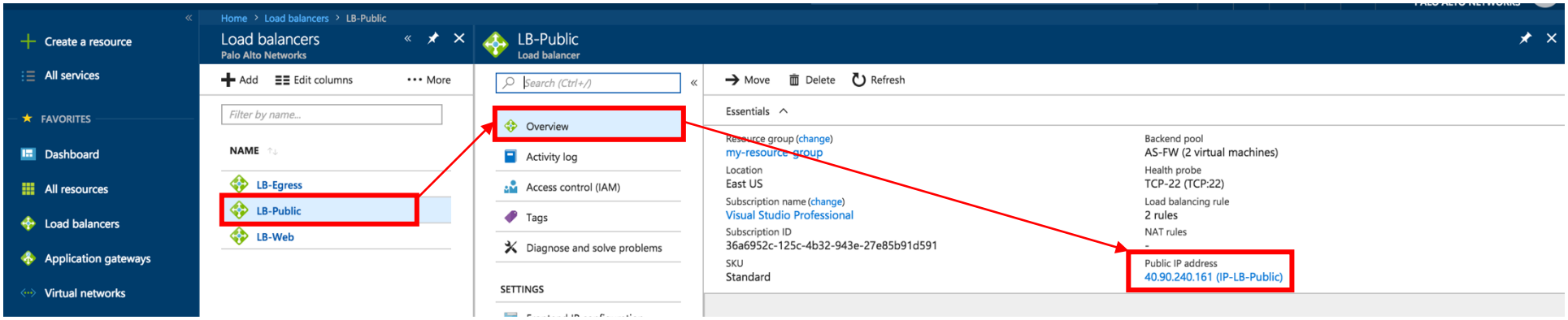


4. Click Load configuration snapshot and select config-fw1
5. Click Commit to apply changes
6. Repeat for VM-FW2 using the config-fw2 configuration file.

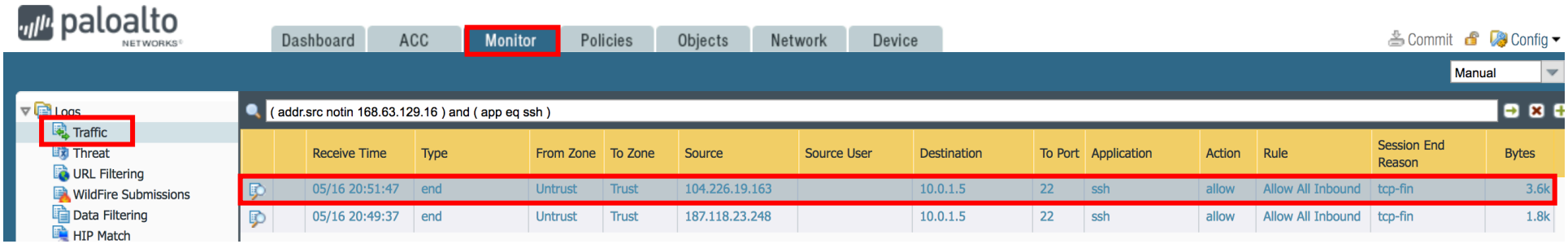


Step 6. Test & view inbound SSH to web servers

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



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.

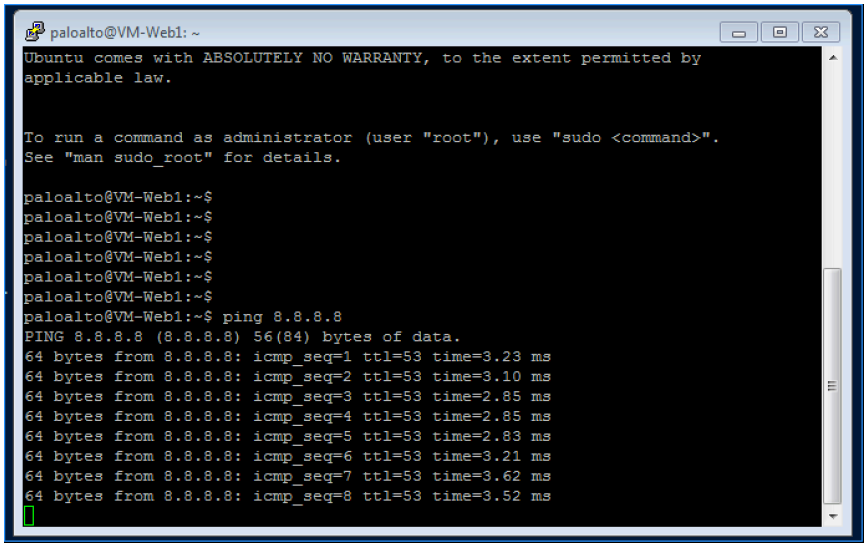


Inbound Final Result

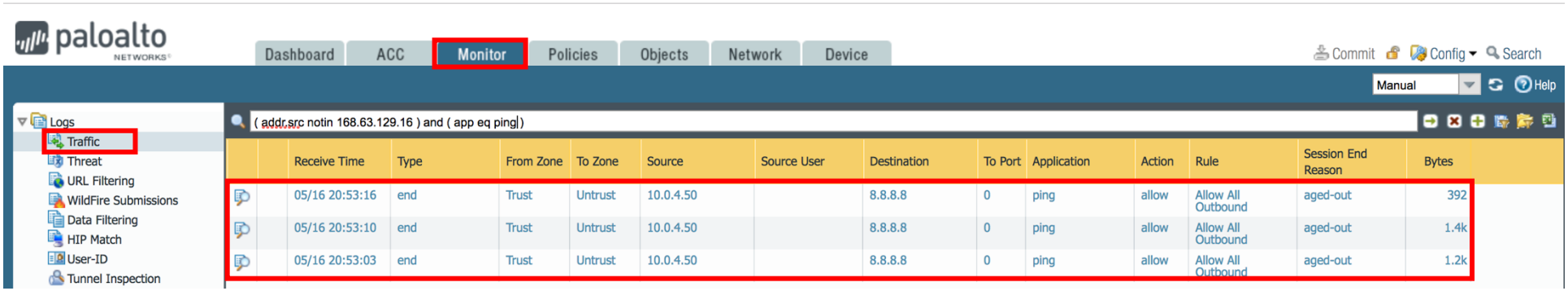
You will see that the SSH session completes to one of the web-servers (10.0.4.50 or 10.0.4.51). The SSH session traverses the Public Load Balancer (LB-Public). The public load balancer sends the session to one of the firewalls. Lastly, the firewall will forward the session to the web-servers load balancer 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.



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



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.