Azure Cloud Framework

Azure Transit VNET Framework Deployment Guide

Date:	**June 20th, 2019**
Revision:	**1.0.a**
Author:	**Dejan Stanic**

This document will detail how to install the Azure Transit VNET Framework demo. The Transit VNET framework will use Panhandler as the deployment tool. The following prerequisites are required to be installed on your local computer prior to the installation of the Azure Transit VNET Framework.

Prerequisites:

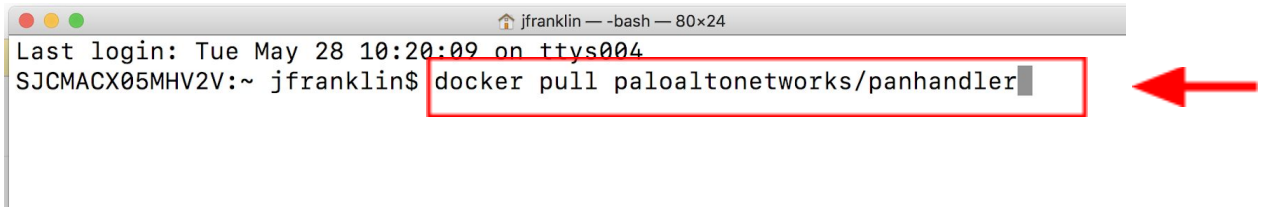
Docker:
Docker will need to be installed to run Panhandler. Here are some links to help with the install:

For Mac:
https://docs.docker.com/docker-for-mac/install/

For Windows:
https://docs.docker.com/docker-for-windows/install/

Panhandler:
Once Docker is installed and running, you will need to pull the panhandler container image from docker hub and build a Panhandler container. From a Mac terminal window or a PC powershell window run the following commands:

docker pull paloaltonetworks/panhandler



After panhandler image is downloaded from Docker Hub, start Panhandler using the following commands:

Mac command:
docker run -t -p 8888:80 -v $HOME:/root/ paloaltonetworks/panhandler &

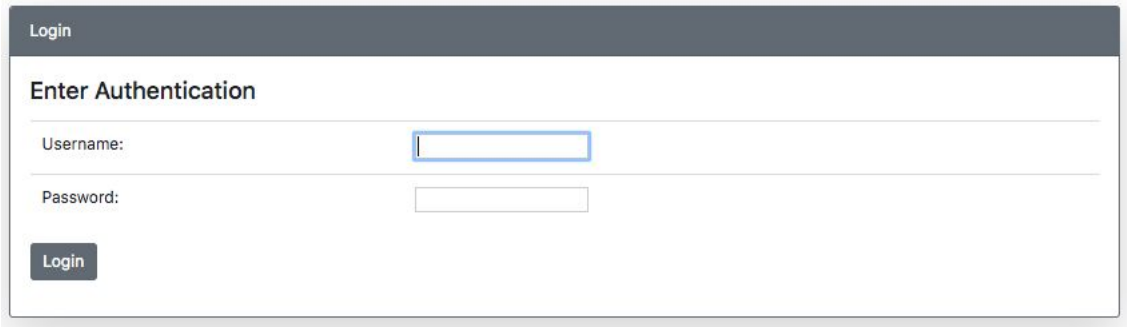
Windows command:
docker run -t -p 8888:80 -v /c/Users/%USERNAME%:/root/ paloaltonetworks/panhandler

```
SJCMACX05MHV2V:~ jfranklin$ docker run -t -p 8888:80 -v $HOME:/root/ paloaltonetworks/panhandler &
[1] 81145
SJCMACX05MHV2V:~ jfranklin$ Adding package panhandler to celery
Adding package panhandler to celery
Adding app config for app: panhandler
```

At this point, you should have a container running on your machine with Panhandler. To access Panhandler, open a browser and navigate to the following URL:

http://localhost:8888

You should see the following login page.

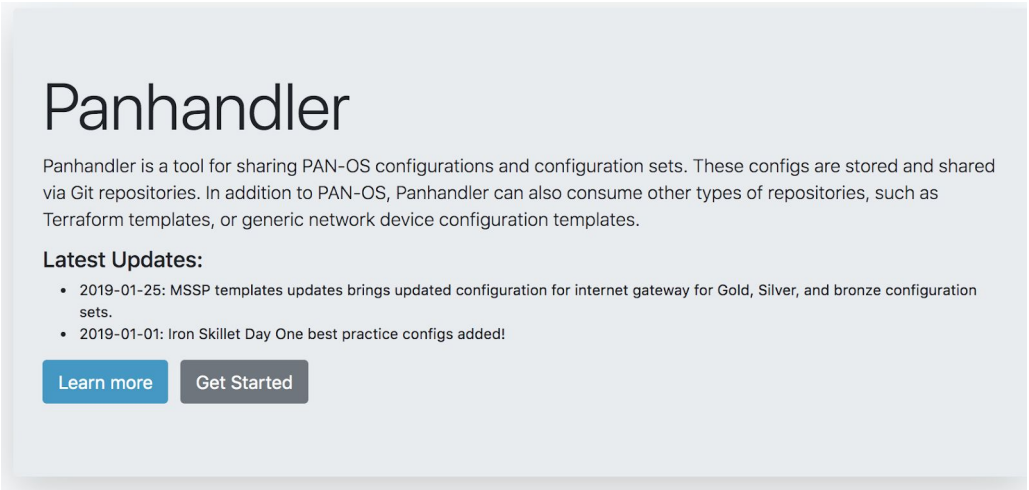


Default login username and password are:

Username: paloalto

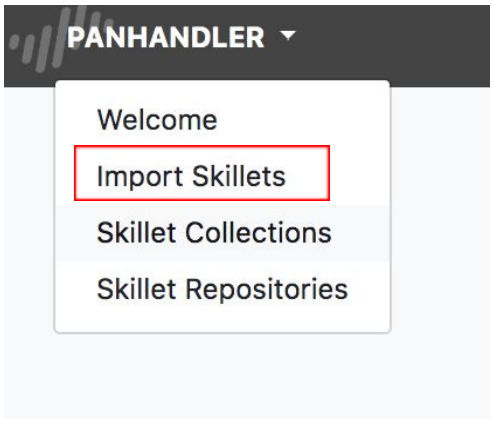
Password: panhandler

Once you are logged in, you will get a welcome screen



Deployment:

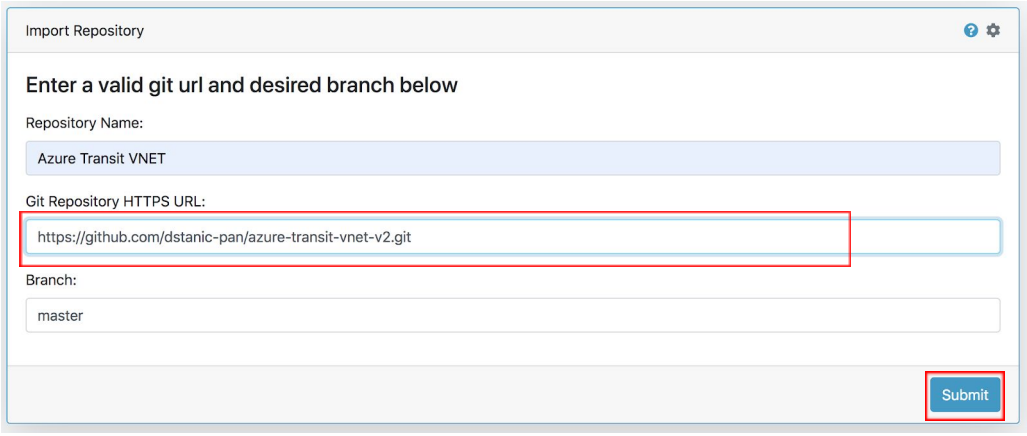
In the upper left hand corner, you will see the Panhandler drop down. Click on the drop down and navigate to the “Import Skillets” option.



To import the Azure Transit VNET Framework, you can scroll down to the Import Repository section, enter Repository Name and Git Repository URL and select Submit button.

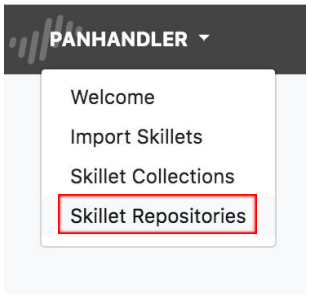
Repository Name: Azure Transit VNET

GitHub URL: https://github.com/dstanic-pan/azure-transit-vnet-v2

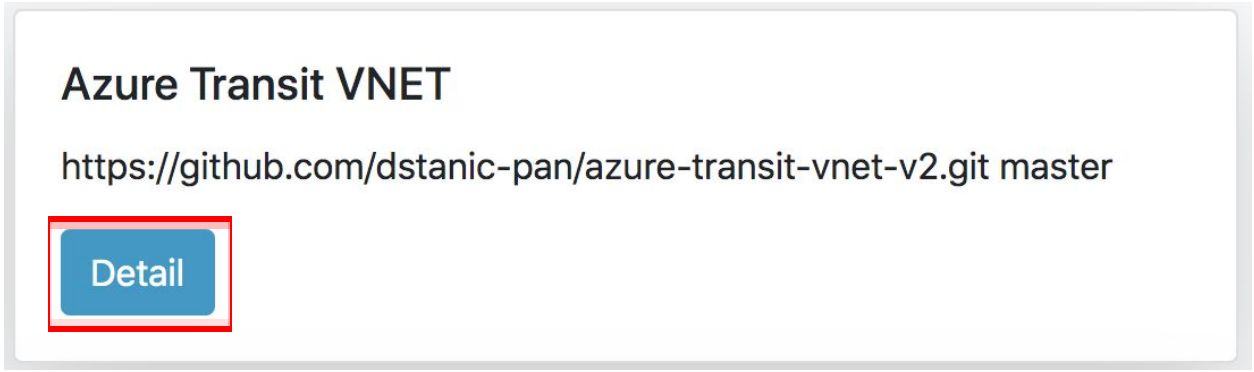


Updates

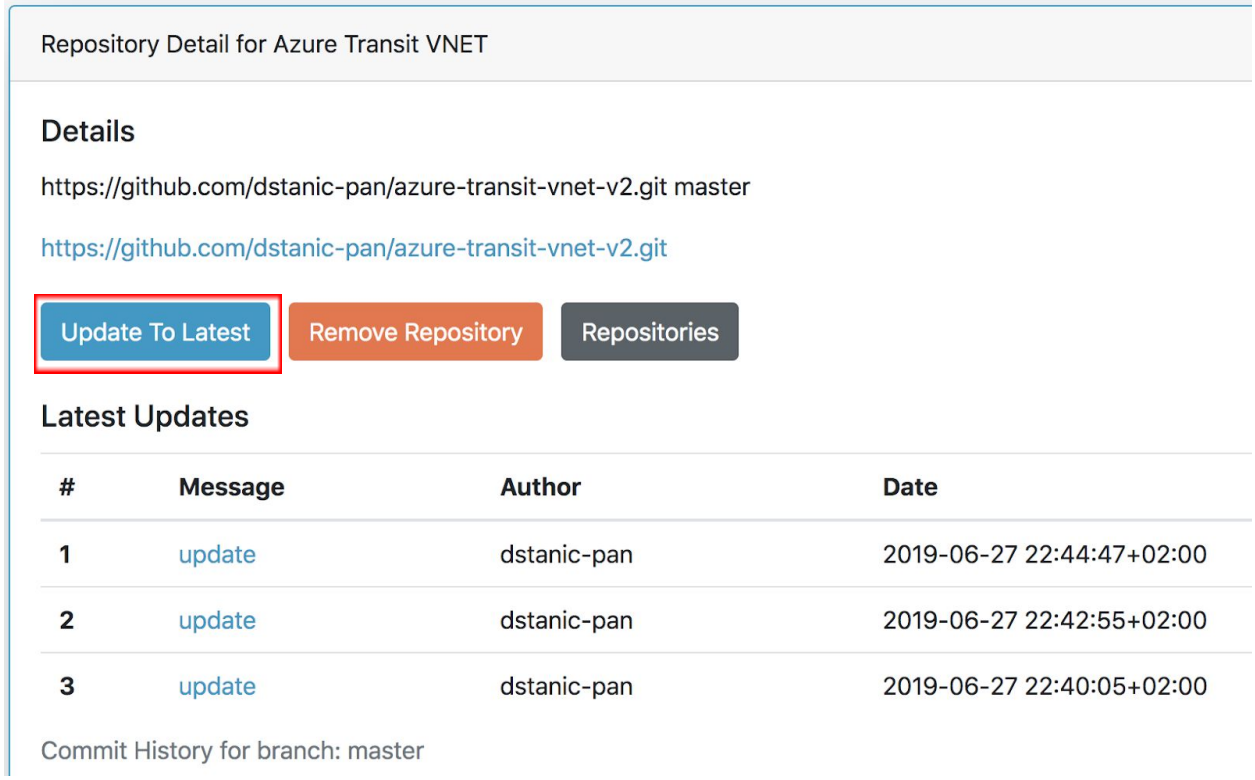
Repositories are periodically updated to include bug fixes or additional functionality. After the initial import, periodically updating the skillets to the latest version is recommended. From the upper left-hand corner Panhandler drop-down list, select “Skillet Repositories”



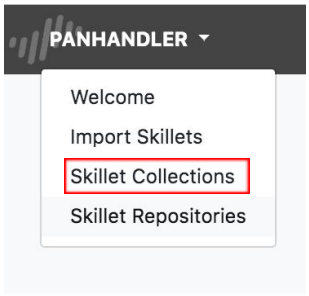
Select Detail under “Azure Transit VNET”:



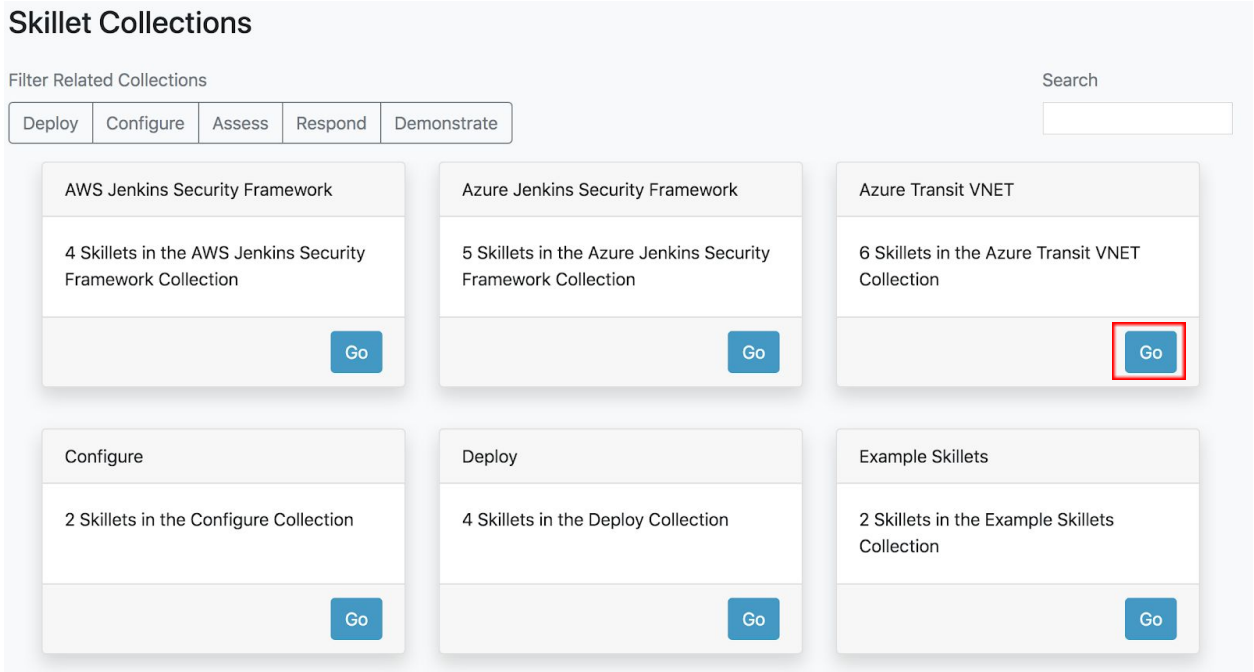
Select Update to Latest:



Once the repository has been added/updated, you are now ready to deploy the demo framework. From the upper left-hand corner Panhandler drop-down list, select “Skillet Collections”



You will see the screen below. Select the Azure Transit VNET



This will take you to the template deployment screen. You will see six options.

Azure Login: In order to run the automation script, you will need to login to the Azure CLI. The Azure login script will launch the login process and provide a URL to connect to and a token to paste into the Azure Website.

Step 1: Infrastructure Deployment - This first step will deploy the Azure architecture, the template will deploy Azure VNets, Route Tables, Subnets, Availability Zones, Load Balancers, Network Security Groups, etc.. The Template will also deploy Palo Alto Networks Firewalls in LB-Sandwich architecture. For a more detailed

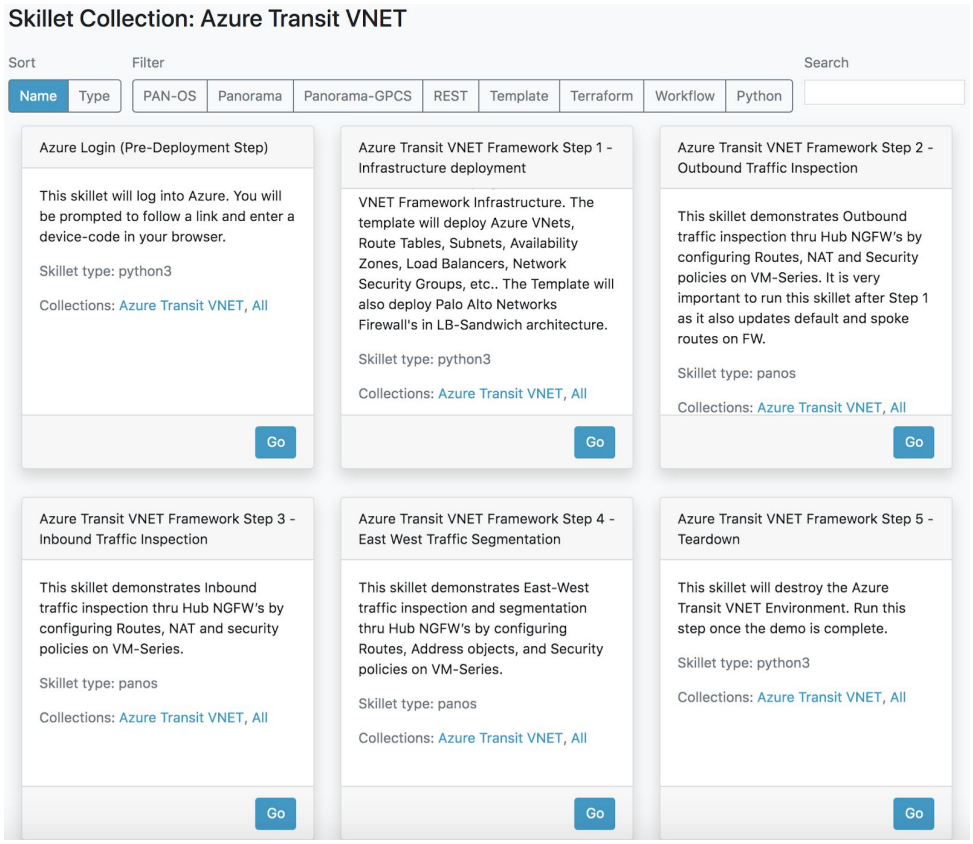
definition of the architecture, please see the “insert link and document name of ppt here”

Step 2: Outbound Traffic Inspection - The second step will configure outbound traffic inspection thru Hub NGFW’s by configuring Routes, NAT and Security policies on VM-Series. It will also finalize initial configuration by updating default and spoke routes on FW’s.

Step 3: Inbound Traffic Inspection - The third step will configure inbound traffic inspection to protected Web1 server by creating corresponding Routes, NAT and Security policies on VM-Series. Traffic will be initiated from internet thru Azure Public LB, NGFW’s and finally web server located in Web subnet of Spoke1 VNET.

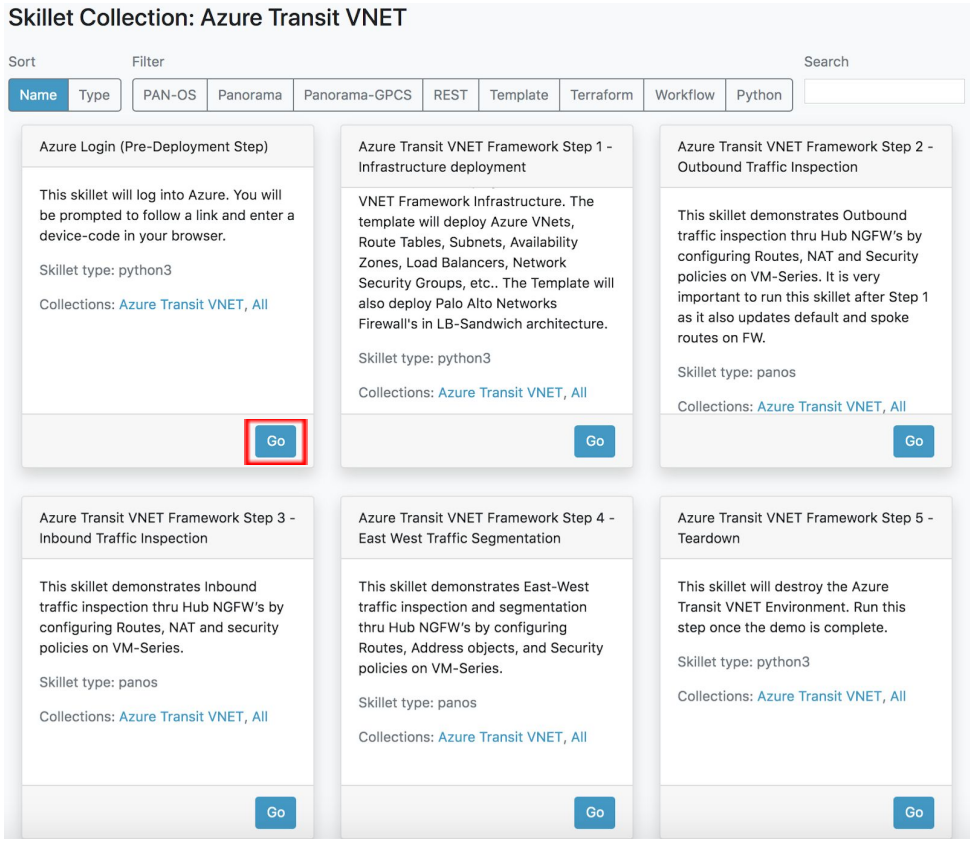
Step 4: East-West Traffic Segmentation - The fourth step will configure East-West traffic inspection and segmentation thru Hub NGFW’s by configuring Routes, Address objects, and Security policies on VM-Series.

Step 5: Once the demo is complete and you are done with the infrastructure, this step will destroy the demo environment.

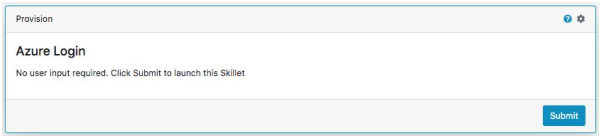


Pre-deployment Login:

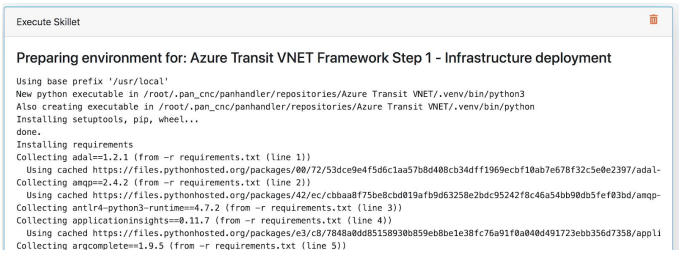
To complete the Azure Login, we are utilizing the Azure CLI login rather than a service principal. The CLI login process will create a token in your home directory that the Panhandler container will use to authenticate the automation templates running in the Panhandler container. To begin the login process, select “Go” on the Azure Login Template box.



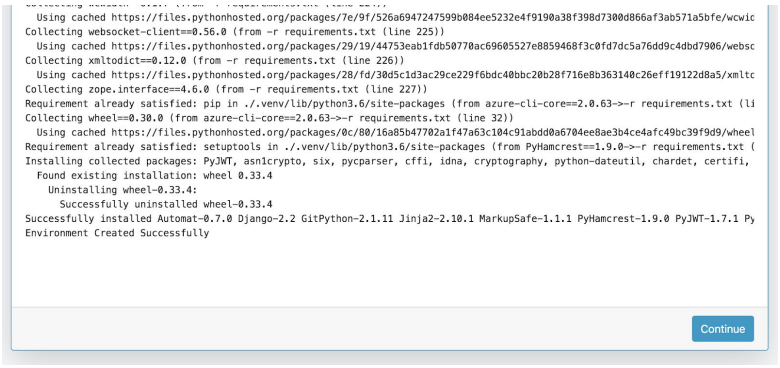
You will see the window below:



Click on the submit button. The first time the demo build is run, Panhandler will validate the correct version of libraries and tools are loaded into the environment. This will only run the first time you deploy the demo and depending on the speed of your internet connection it can take up to 10 minutes to complete. Below is the screen that you will see during the environment verification:



Once the environment verification is completed, (blue continue button will indicate the process is complete) you will see the following:

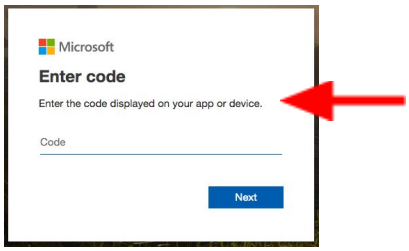


Click on the Continue button.

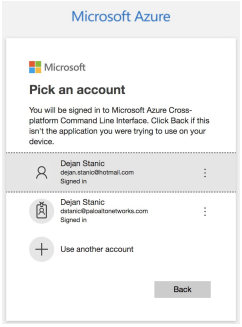
The CLI login process will generate a security code that will need to be copied and pasted into the URL listed in the window. Each time the login process is run, new security code and token will be generated. Navigate to the URL in a browser on your computer:

https://microsoft.com/devicelogin

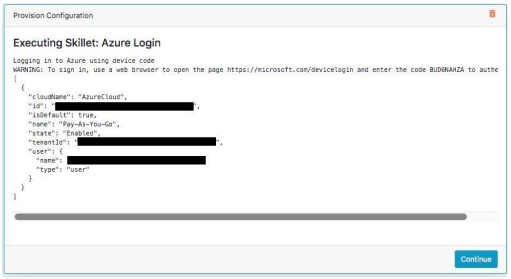
From the Microsoft website opened in your browser, enter your code into the site



You will then select the account you would like to login into Azure. You can use a personal account or the corporate account. Click on the account and the login process will be completed.



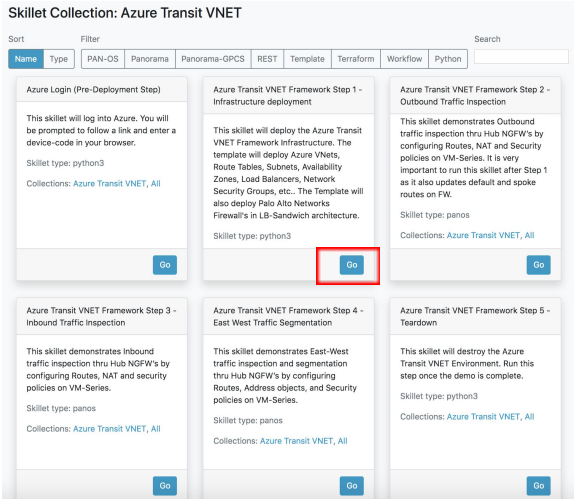
Once you log into Azure from the website, if you go back to Panhandler, you will see that Panhandler has picked up your login and will display the login as below:



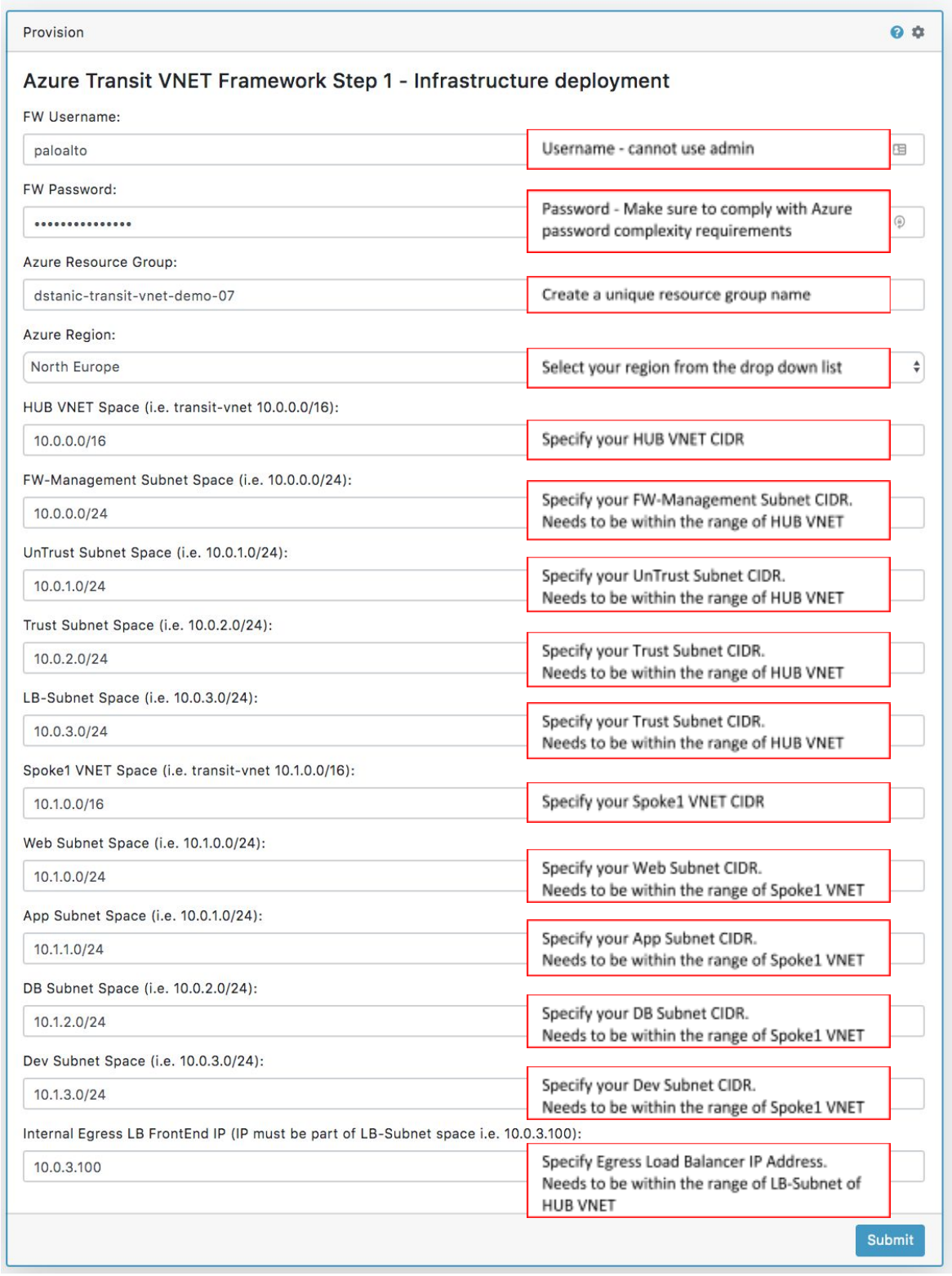
Select Continue and you will be taken back to the main Azure Transit VNET Framework Window.

Launch Step 1: (Infrastructure deployment)

Click on the Go button on the step 1 deployment template.

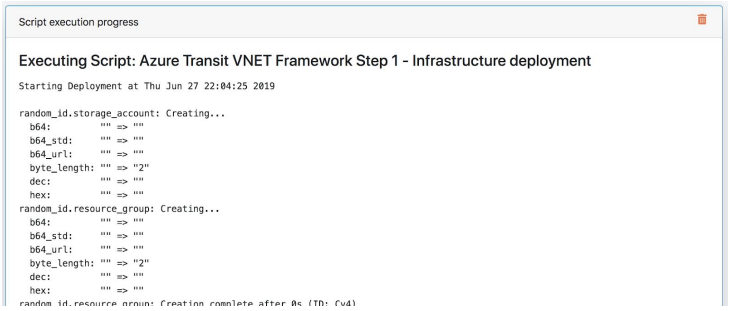


You should see the following screen:



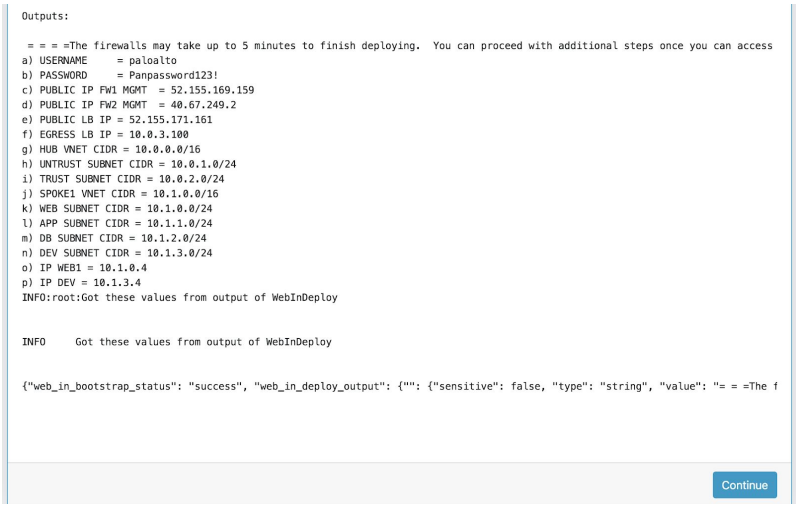
Once the above information is added, select the Submit button to begin the installation.

Select the Continue button from the screen above and it will immediately start the build of the Azure Transit VNET Infrastructure, as shown below.



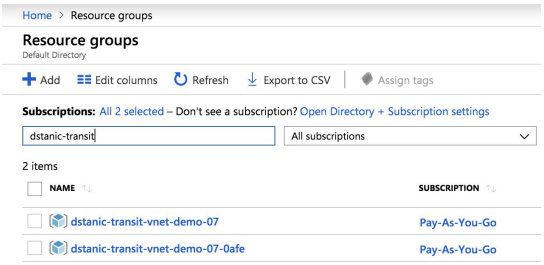
The build of the architecture will take approximately 8 - 10 minutes.

Once the Infrastructure build is complete, you will see the following:



Copy deployment Output values into the text editor and select Continue from the screen above to take you back to the main Azure Transit VNET Framework page.

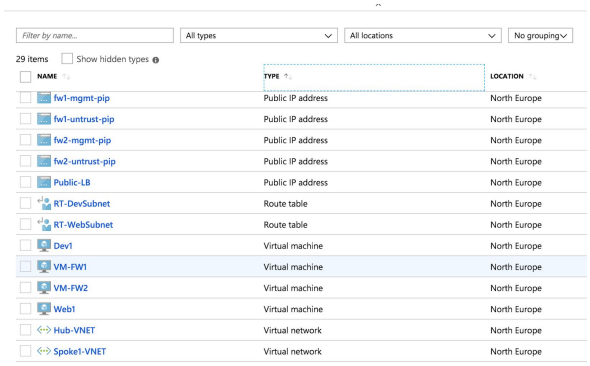
Now is a great time to login to your Azure environment and review deployed infrastructure.



As you can see above, the deployment process created two Resource Groups:

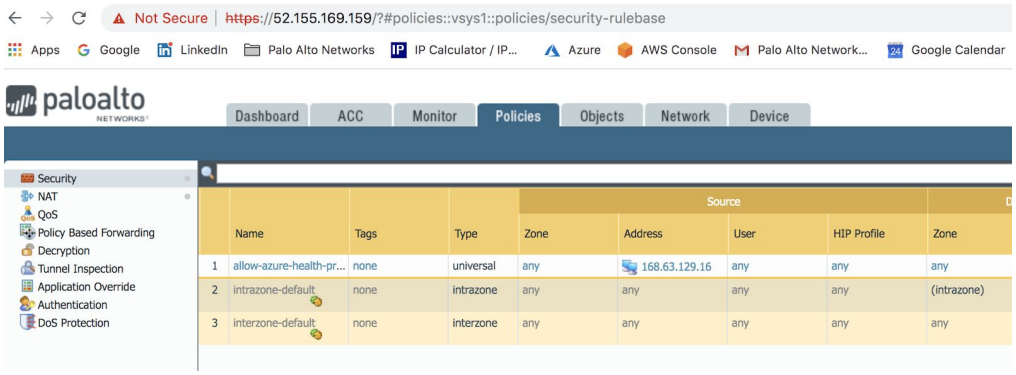
dstanic-transit-vnet-demo-07-0afe - used for bootstrapping, hosts Storage account with Fileshare

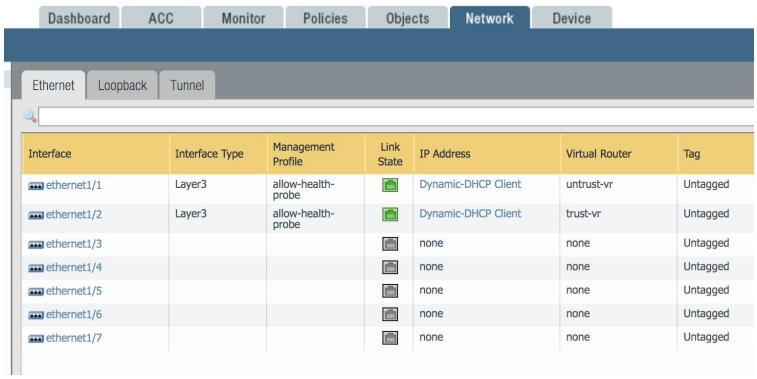
dstanic-transit-vnet-demo-07 - all infrastructure resources are deployed in here



NAME	TYPE	LOCATION
fw1-mgmt-pip	Public IP address	North Europe
fw1-untrust-pip	Public IP address	North Europe
fw2-mgmt-pip	Public IP address	North Europe
fw2-untrust-pip	Public IP address	North Europe
Public-LB	Public IP address	North Europe
RT-DevSubnet	Route table	North Europe
RT-WebSubnet	Route table	North Europe
Dev1	Virtual machine	North Europe
VM-FW1	Virtual machine	North Europe
VM-FW2	Virtual machine	North Europe
Web1	Virtual machine	North Europe
Hub-VNET	Virtual network	North Europe
Spoke1-VNET	Virtual network	North Europe

The best way to ensure that FW's are ready for the next step is to login to the management console. Select PUBLIC IP FW1 MGMT, PUBLIC IP FW2 MGMT from output values and paste the IP's into your web browser. If needed, credentials can also be found in the Outputs. While reviewing Policies, Objects and Network tabs you will notice that only very basic configuration was loaded and that we are missing some Routes, Objects, Security and NAT policies. This is desired configuration as we will configure our FW's to enable different use-cases in Steps 2, 3 and 4.



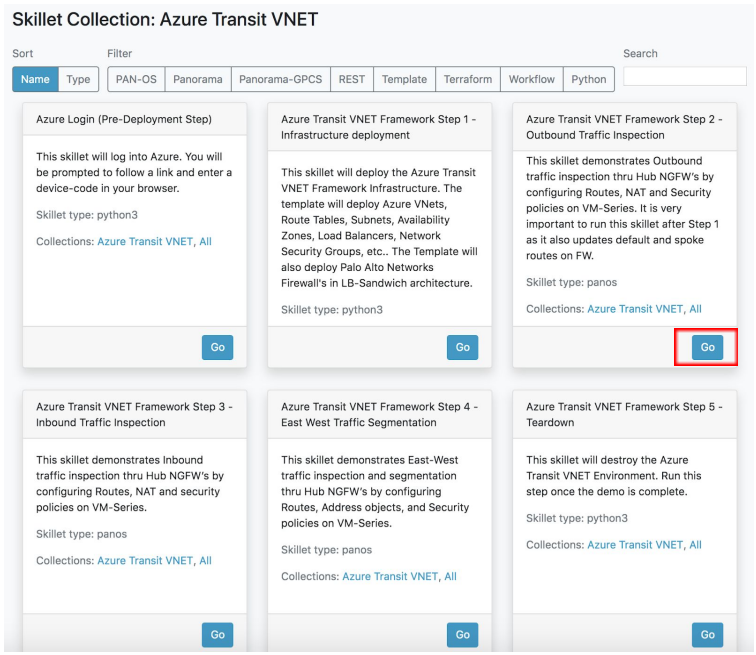


You are now ready to run the first use-case and secure outbound traffic.
Launch Step 2: (Outbound traffic inspection)

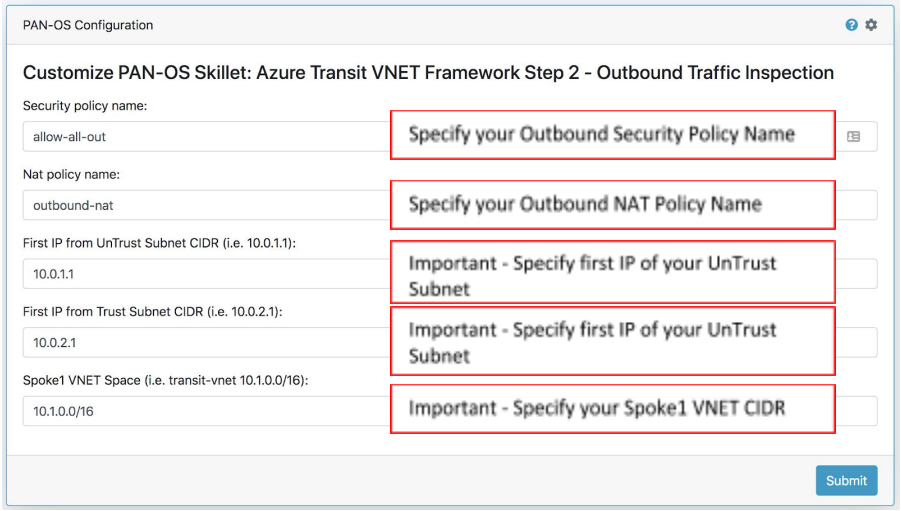
During the deployment process, we have deployed two Linux test instances Web1 and Dev1 in corresponding subnets of Spoke1-VNET. Before launching the Step 2 login to your Dev1 instance and try to access public resources (i.e. wget www.google.com or ping 8.8.8.8).

You will notice that at this stage it is not possible to reach them out.

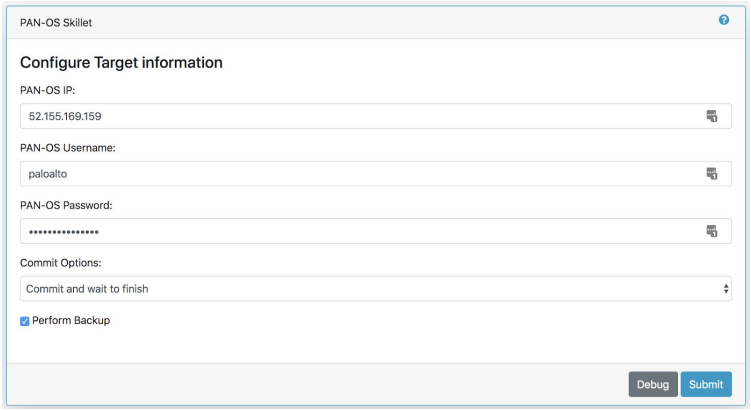
To initiate Step 2 go back to the Panhandler, Click on the Go button on the step 2 Outbound Traffic Inspection deployment template.



This will launch the inputs page. You should see the following screen:

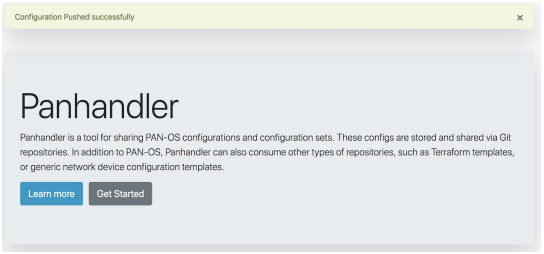


Once the selection is complete, click “Submit” to initiate the configuration process.



Provide the FW1 details (all details can be found in output values), click “Submit” to initiate API calls that will create Routes, Security and NAT Rules to enable Outbound traffic.

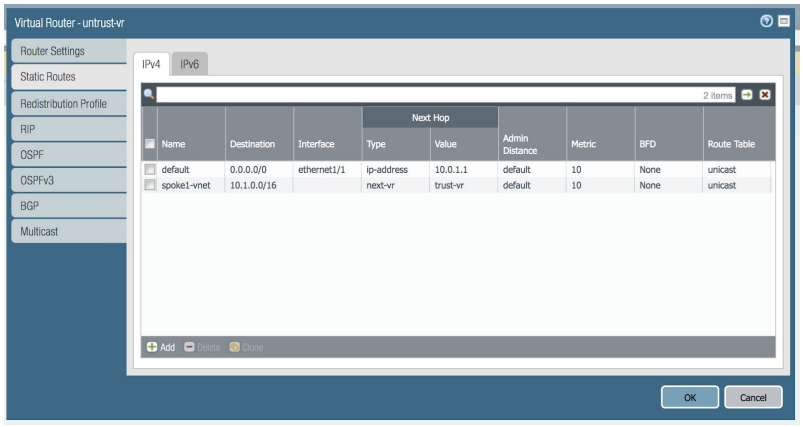
Once the process is complete, you will see the following:



Repeat the process to configure FW2. To simplify the process, select Back in your browser, change PAN-OS IP value to FW2, provide your password and click “Submit”.

Go back to your FW1 and FW2 management console and review Virtual Routers untrust-vr and trust-vr, Security and NAT policies.

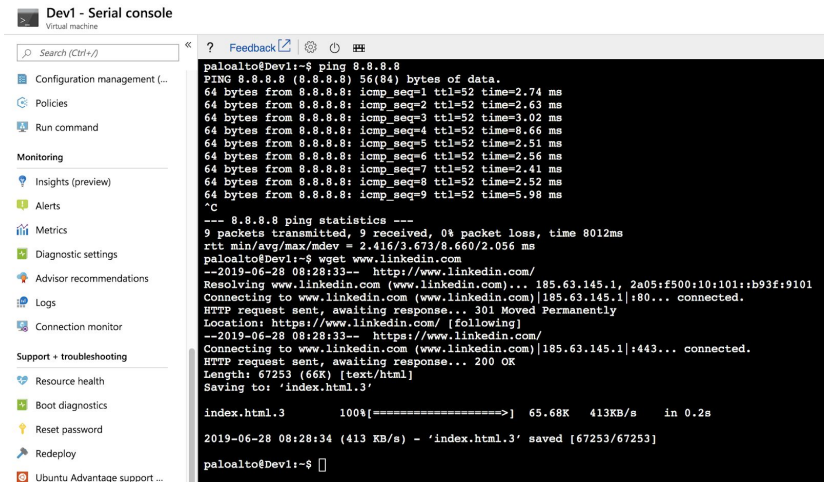
Virtual Router:



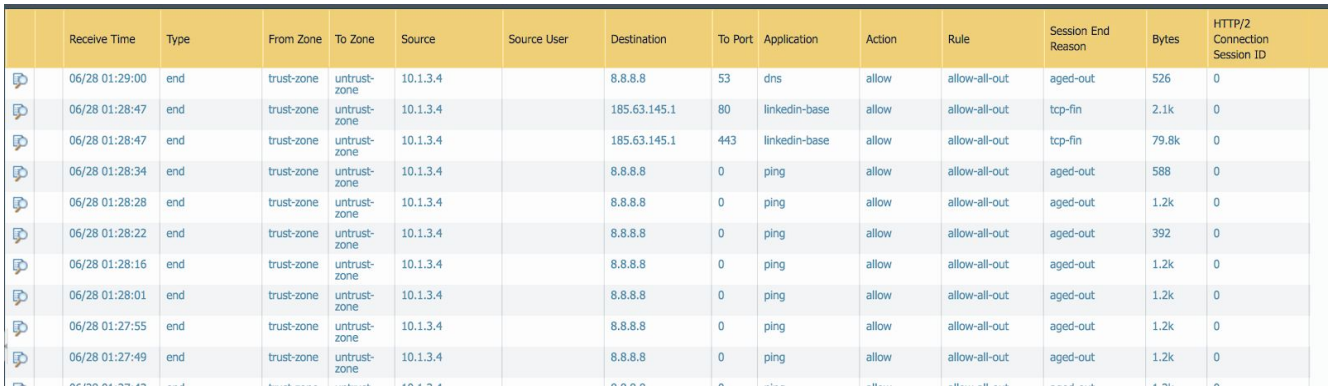
Security Policies:

NAT Rules:

Login to your Dev1 instance and try again to access public resources (i.e. wget www.google.com or ping 8.8.8.8). This time you should be able to access public resources.



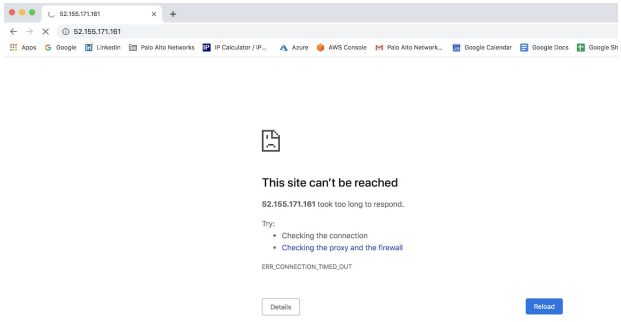
Select the Monitor tab on FW1 and FW2 and review the traffic log. You should see similar to the picture below.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
	06/28 01:29:00	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	53	dns	allow	allow-all-out	aged-out	526	0
	06/28 01:28:47	end	trust-zone	untrust-zone	10.1.3.4		185.63.145.1	80	linkedin-base	allow	allow-all-out	tcp-fin	2.1k	0
	06/28 01:28:47	end	trust-zone	untrust-zone	10.1.3.4		185.63.145.1	443	linkedin-base	allow	allow-all-out	tcp-fin	79.8k	0
	06/28 01:28:34	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	588	0
	06/28 01:28:28	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	1.2k	0
	06/28 01:28:22	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	392	0
	06/28 01:28:16	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	1.2k	0
	06/28 01:28:01	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	1.2k	0
	06/28 01:27:55	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	1.2k	0
	06/28 01:27:49	end	trust-zone	untrust-zone	10.1.3.4		8.8.8.8	0	ping	allow	allow-all-out	aged-out	1.2k	0

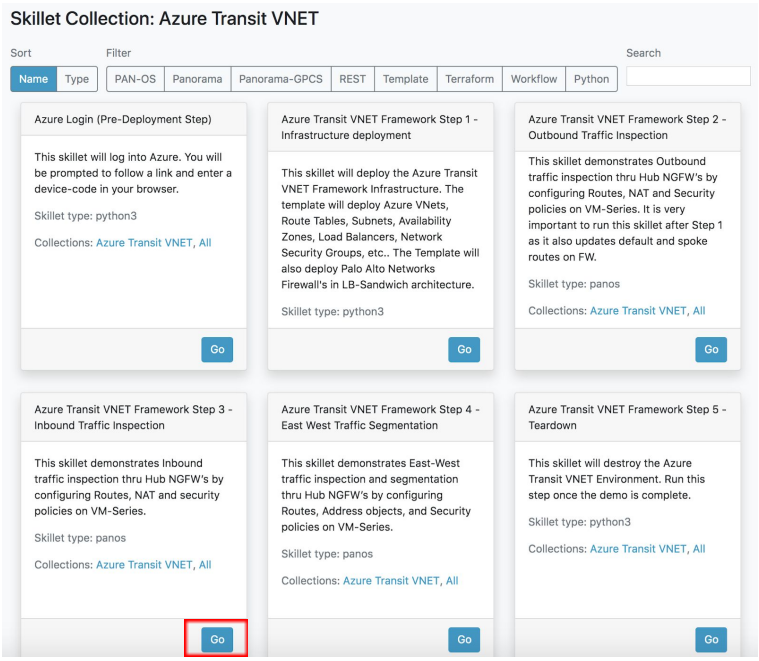
Launch Step 3: (Inbound traffic inspection)

During the deployment process, we have deployed Web1 with Apache web server in Spoke1-VNET. Before launching the Step 3 select PUBLIC LB IP from output values and paste the IP's into your web browser.

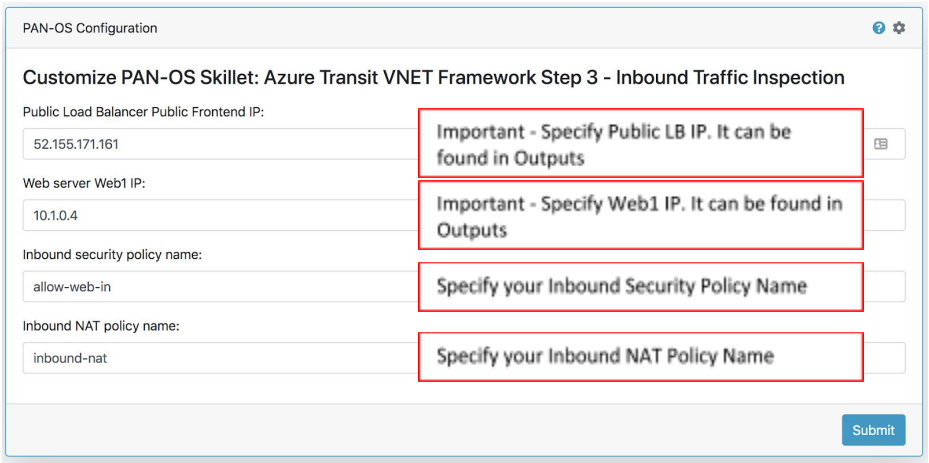


You will notice that at this stage it is not possible to reach out your Web1 server.

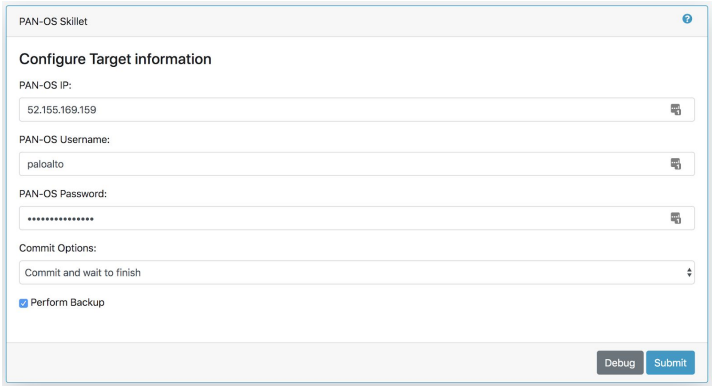
To initiate Step 3 go back to the Panhandler, Click on the Go button on Step 3 Inbound Traffic Inspection deployment template.



This will launch the inputs page. You should see the following screen:

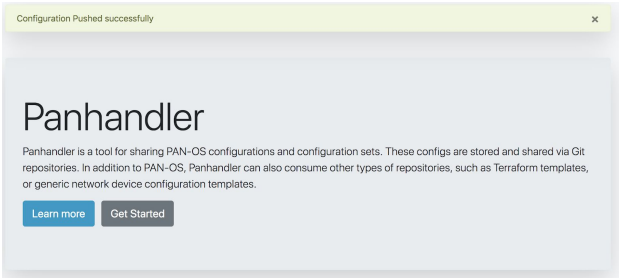


Once the selection is complete, click “Submit” to initiate the configuration process.



Provide the FW1 details (all details can be found in output values), click “Submit” to initiate API calls that will create Objects, Security and NAT Rules to enable Inbound traffic.

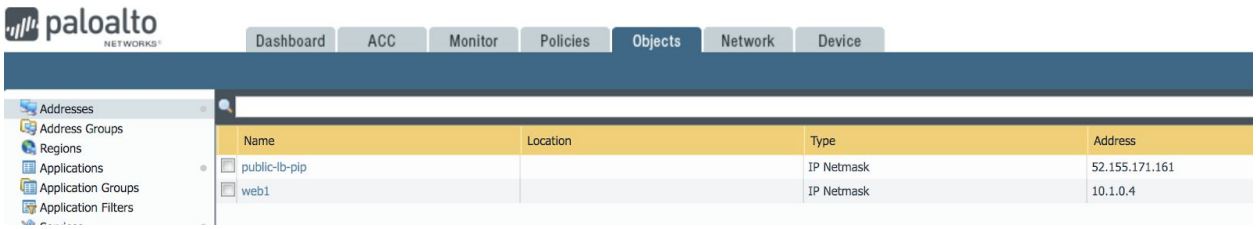
Once the process is complete, you will see the following:



Repeat the process to configure FW2. To simplify the process, select Back in your browser, change PAN-OS IP value to FW2, provide your password and click “Submit”.

Go back to your FW1 and FW2 management console and review Address objects, Security and NAT policies.

Address objects:



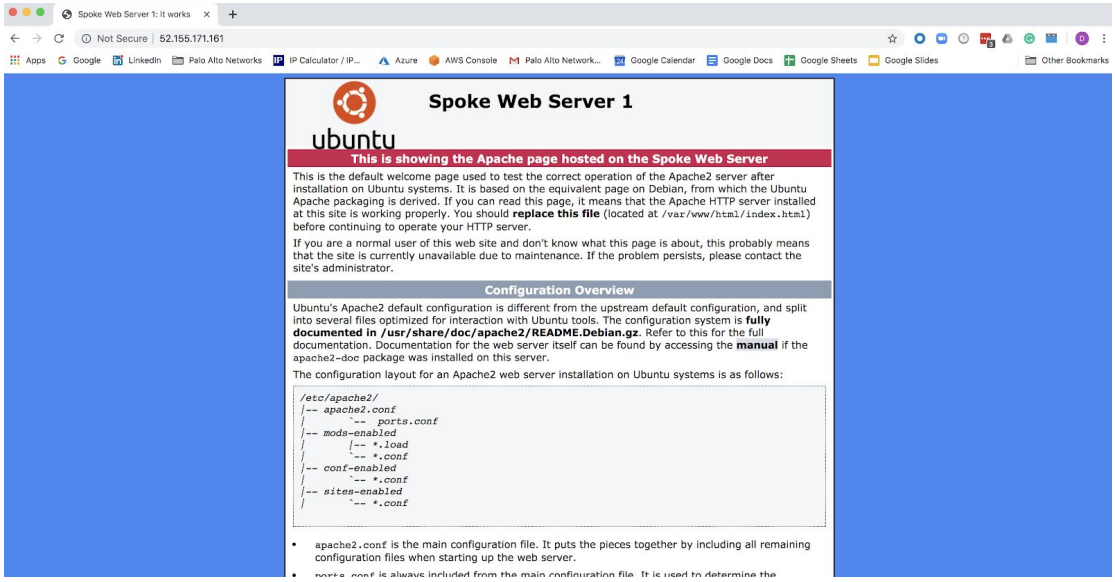
Security Policies:

	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	allow-azure-health-pr...	none	universal	any	168.63.129.16	any	any	any	any	ssh	application-d...	Allow	none
2	allow-all-out	none	universal	trust-zone	any	any	any	untrust-zone	any	any	any	Allow	
3	allow-web-in	none	universal	untrust-zone	any	any	any	trust-zone	any	web-browsing	application-d...	Allow	none

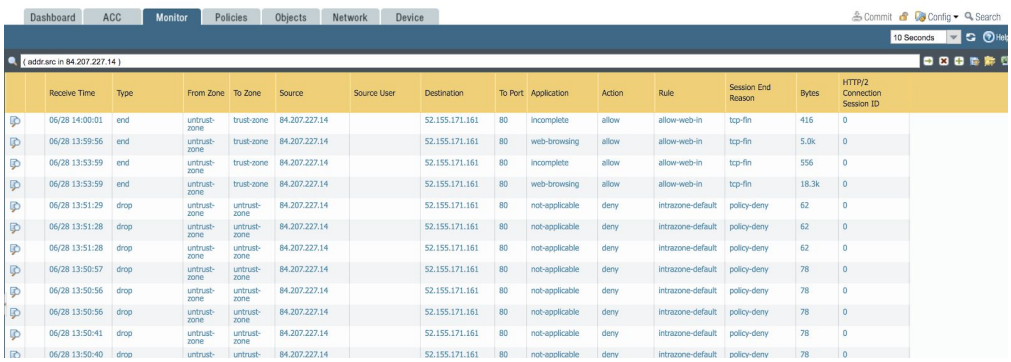
NAT Rules:

			Original Packet						Translated Packet		
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count
1	azure-probe-no-nat	none	untrust-zone	untrust-zone	any	168.63.129.16/...	any	any	none	none	5380
2	outbound-nat	none	trust-zone	untrust-zone	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	1642
3	inbound-nat	none	untrust-zone	untrust-zone	any	any	public-lb-pip	any	none	destination-translation address: web1 port: 80	6

Refresh your browser with PUBLIC LB IP from output values. This time you should see the following:

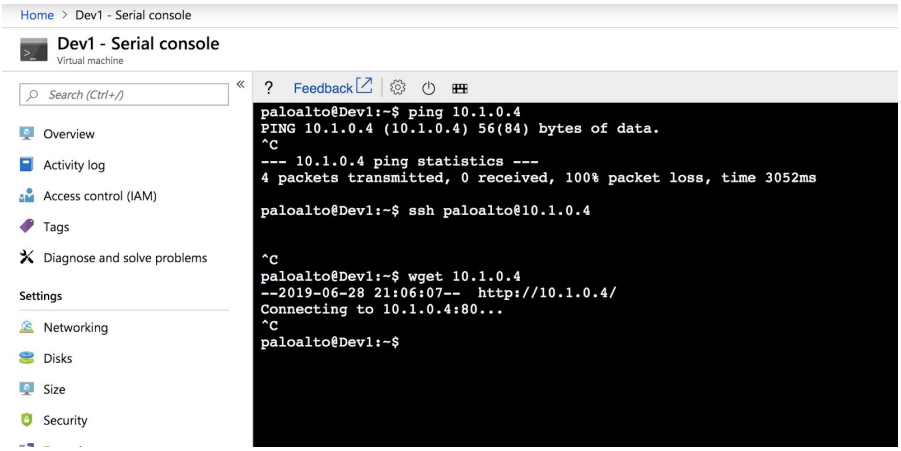


Select the Monitor tab on FW1 and FW2 and review the traffic log. You should see similar to the picture below.



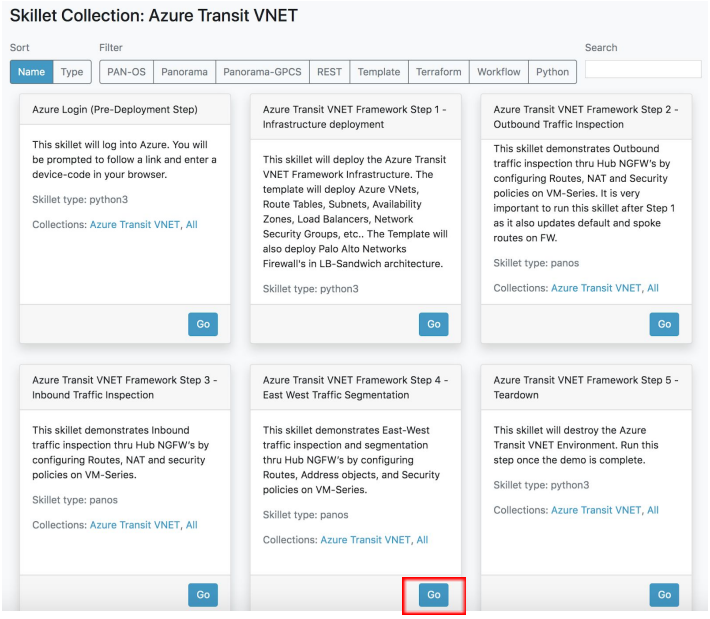
Launch Step 4: (East-West traffic inspection and segmentation)

During the deployment process, we have deployed two Linux test instances in Spoke1-VNET Web1 in Web Subnet and Dev1 in Dev Subnet. Before launching the Step 4 login to your Dev1 instance and try to ping, ssh and wget your Web1 instance.

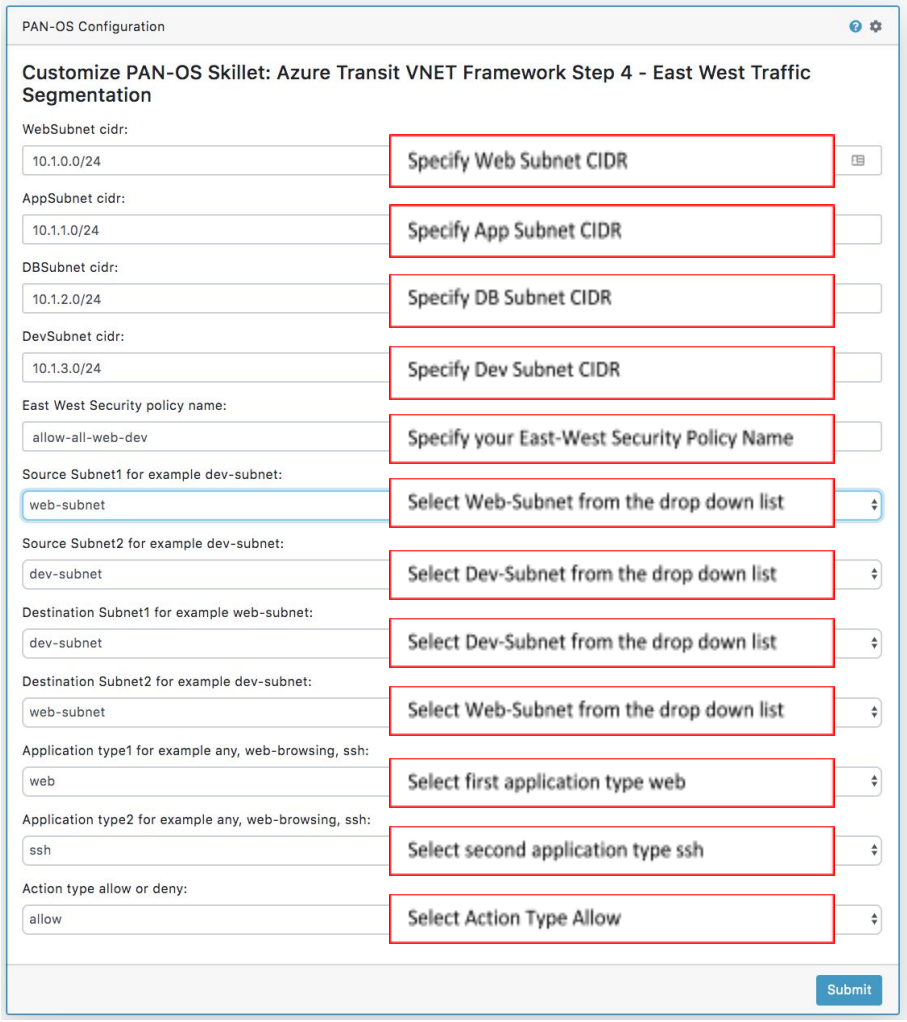


You will notice that at this stage it is not possible to reach Web1.

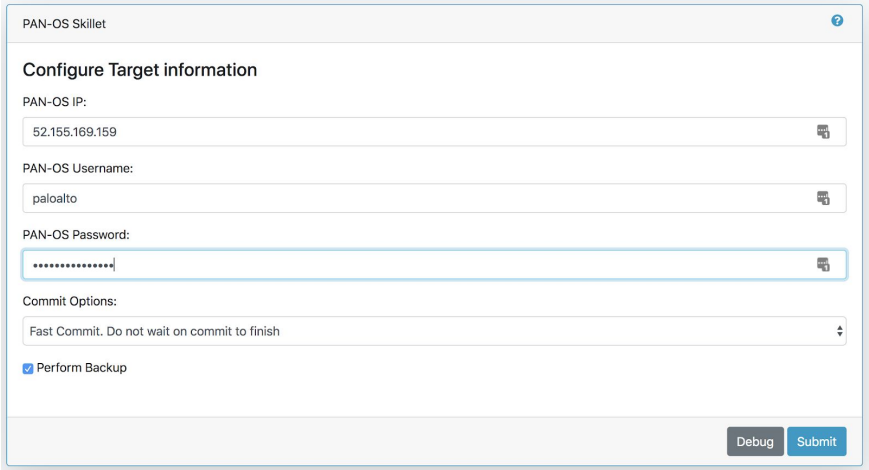
To initiate the Step 4 go back to the Panhandler, Click on the Go button on Step 4 - East-West Traffic Segmentation deployment template. This will launch the inputs page.



You should see the following screen:

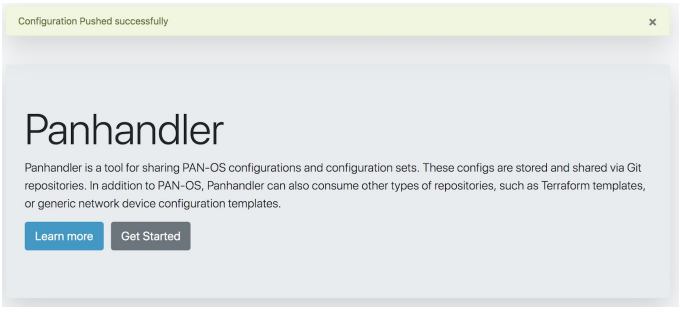


Once the selection is complete, click “Submit” to initiate the configuration process.



Provide the FW1 details (all details can be found in output values), click “Submit” to initiate API calls that will create Objects and Security policies to enable East-West ssh and web traffic between Web and Dev subnets.

Once the process is complete, you will see the following:

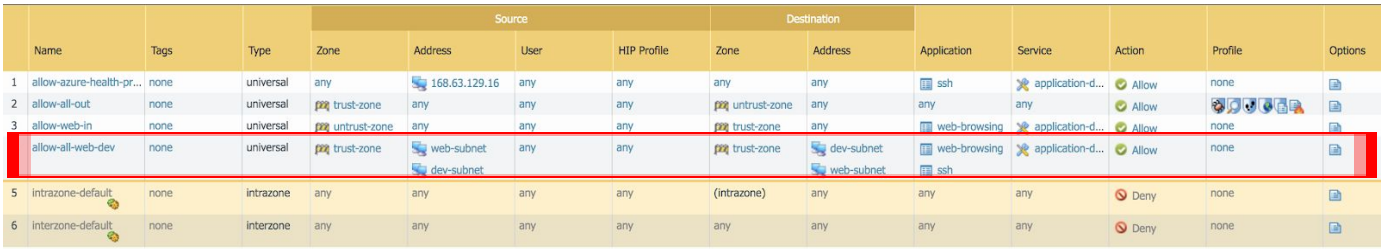


Repeat the process to configure FW2. To simplify the process, select Back in your browser, change PAN-OS IP value to FW2, provide your password and click “Submit”.

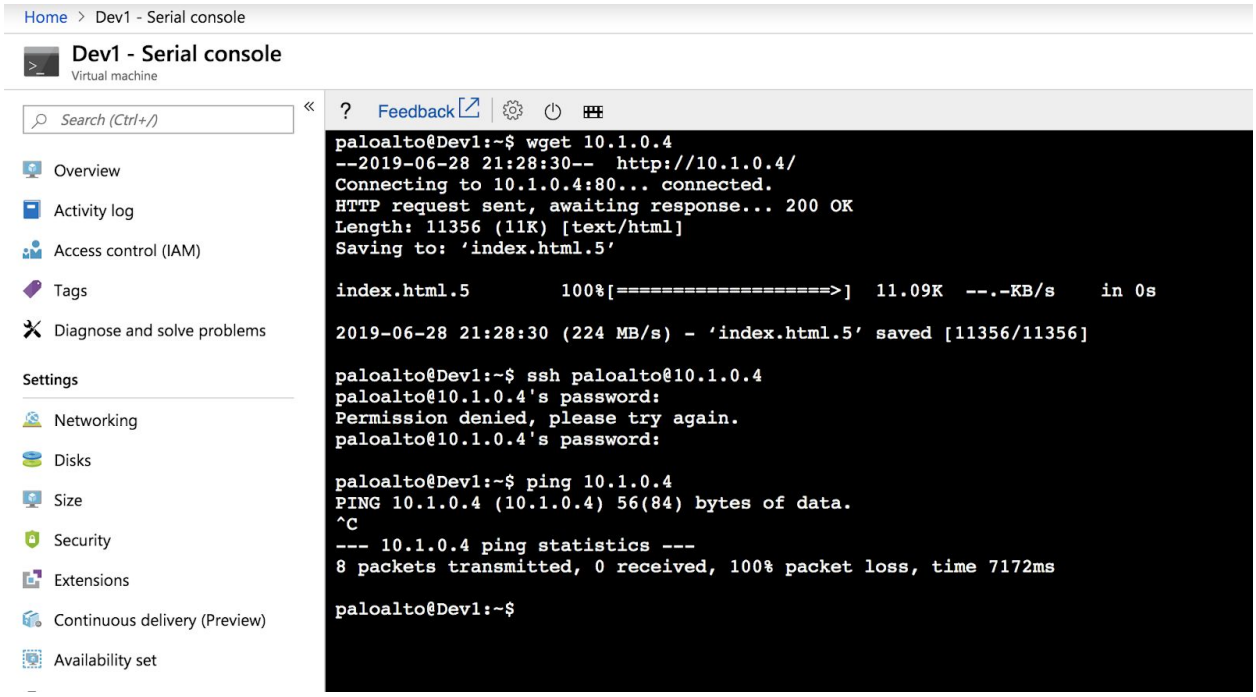
Go back to your FW1 and FW2 management console and review Address objects and Security policies.

Address Objects:

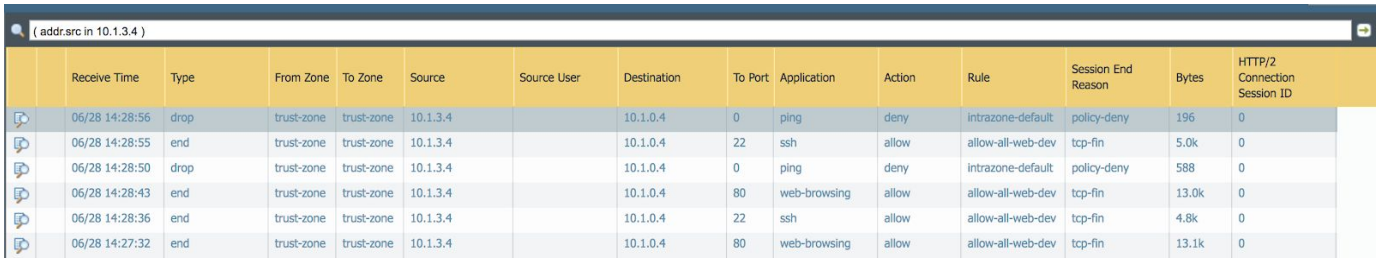
Security Policies:



Login to your Dev1 instance and try again to ping, ssh and wget your Web1 instance. You should be able to wget and ssh but not to ping. This is because we created a security policy that only allows ssh and web-browsing between Dev and Web Subnets.



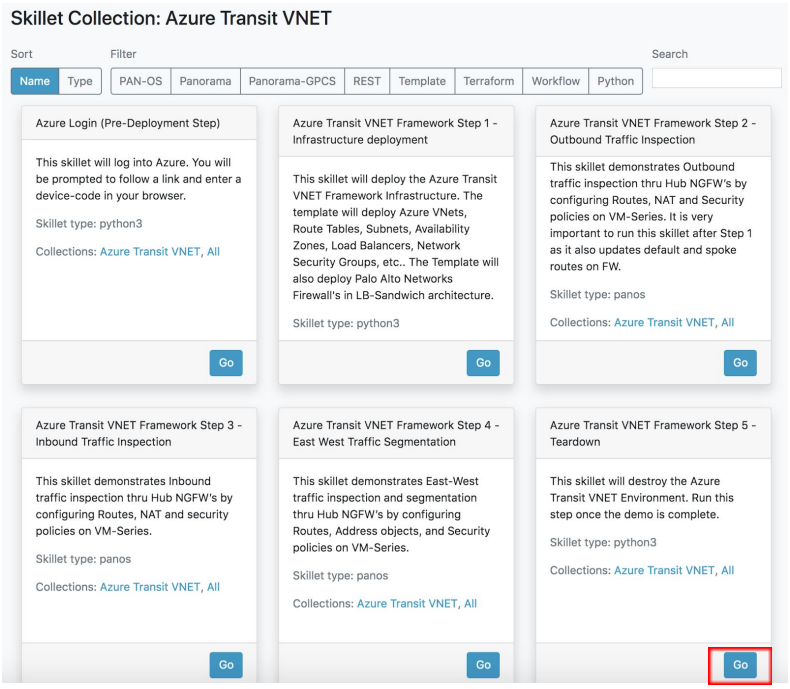
Select the Monitor tab on FW1 and FW2 and review the traffic log. You should see similar to the picture below.



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection Session ID
	06/28 14:28:56	drop	trust-zone	trust-zone	10.1.3.4		10.1.0.4	0	ping	deny	intrazone-default	policy-deny	196	0
	06/28 14:28:55	end	trust-zone	trust-zone	10.1.3.4		10.1.0.4	22	ssh	allow	allow-all-web-dev	tcp-fin	5.0k	0
	06/28 14:28:50	drop	trust-zone	trust-zone	10.1.3.4		10.1.0.4	0	ping	deny	intrazone-default	policy-deny	588	0
	06/28 14:28:43	end	trust-zone	trust-zone	10.1.3.4		10.1.0.4	80	web-browsing	allow	allow-all-web-dev	tcp-fin	13.0k	0
	06/28 14:28:36	end	trust-zone	trust-zone	10.1.3.4		10.1.0.4	22	ssh	allow	allow-all-web-dev	tcp-fin	4.8k	0
	06/28 14:27:32	end	trust-zone	trust-zone	10.1.3.4		10.1.0.4	80	web-browsing	allow	allow-all-web-dev	tcp-fin	13.1k	0

Launch Step 5:

Click on the Go button on the Step 5 deployment template. This will clean up the environment, destroying everything thus far created.



You should see the following screen:

Select Submit. Note that this process will take several minutes to complete. The process is complete when you get the “Continue” button at the bottom of the page.