

FORTIGATE

Microsoft Azure Test Drive



Test Drive Guide

Updated: December 15th, 2021

Fortinet FortiGate – Azure Test Drive

TABLE OF CONTENTS

FORTIGATE TEST DRIVE	3
How to use this guide	3
About the test drive environment	3
TASK 1 – Connect to FortiGate & Webserver	4
TASK 2 – Add outbound connectivity Policy.....	8
TASK 3 – Install Apache2 Webserver	10
TASK 4 – Configure FortiGate for web traffic	10
TASK 5 – Connect to Webserver.....	13

FORTIGATE

TEST DRIVE

This test drive will allow you to experience how a FortiGate firewall enables enterprises to control their resources and applications in Microsoft Azure through Fortinet solutions. Fortinet solutions provide the freedom to deploy any application on Microsoft Azure without compromising security.

HOW TO USE THIS GUIDE

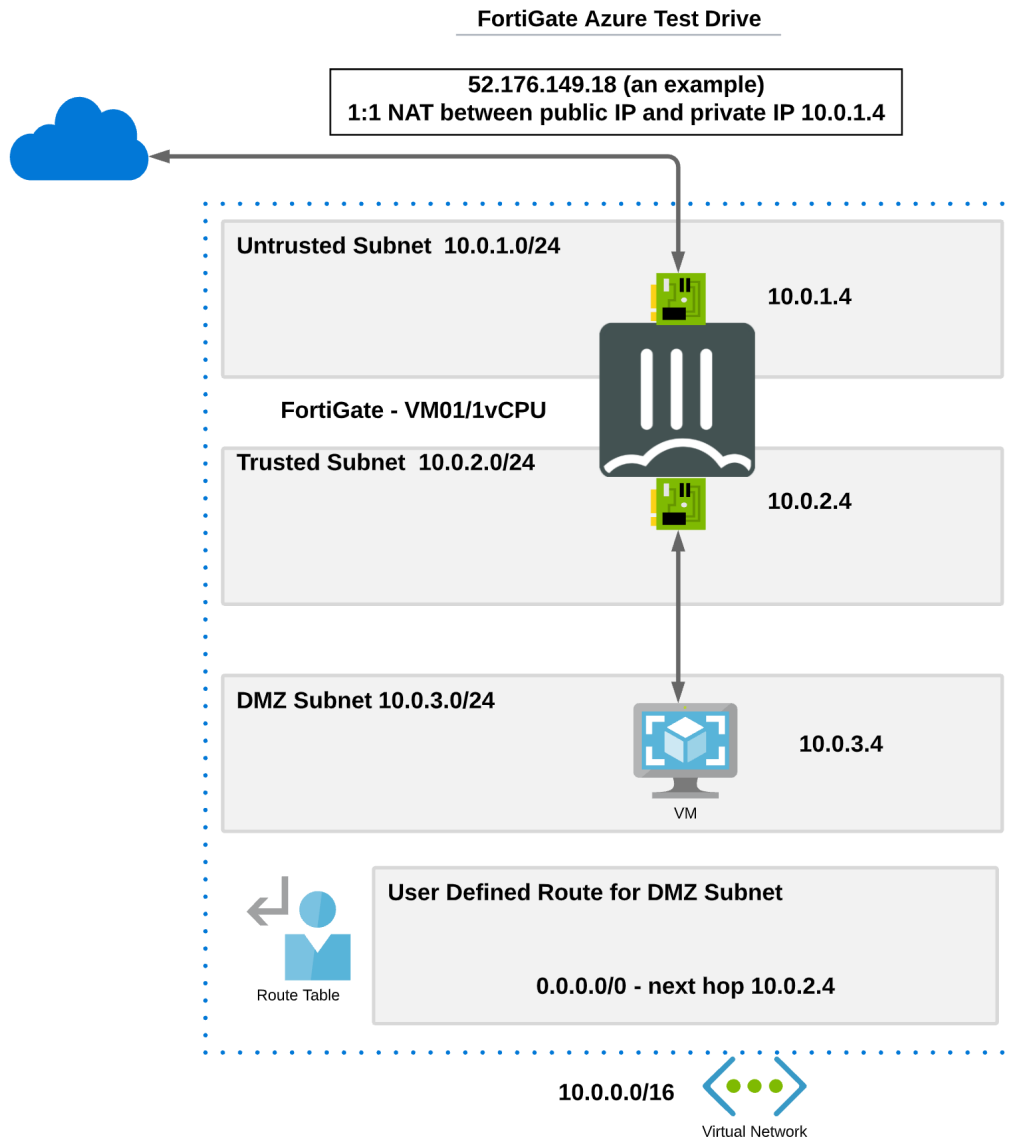
The activities outlined in this test drive guide contain all the information necessary to complete the defined scenarios and outlined tasks. Only a web browser is required to complete the test drive.

ABOUT THE TEST DRIVE ENVIRONMENT

You will configure Firewall policies on the FortiGate-VM firewall via the FortiGate GUI to install and enable a webserver hosted in Azure access to the Internet and then enable Virtual IPs to provide secured access

Fortinet FortiGate – Azure Test Drive

from your device to the webserver hosted in Azure and protected by the FortiGate.




TASK 1 – CONNECT TO FORTIGATE & WEBSERVER


1. When the Test Drive is ready **click** on the FortiGate link to open the GUI.

Fortinet FortiGate – Azure Test Drive

Microsoft | Azure Marketplace | Apps | Consulting Services | Hire an expert | Search Marketplace

Apps > FortiGate NGFW - Single VM with ARM Template > Test Drive

 FortiGate NGFW - Single VM with ARM Template
Test Drive
by Fortinet

 **Your Test Drive is ready** (2 hours 56 minutes remaining)

To use this Test Drive, please follow the "Test Drive User Manual" link below to obtain a step-by-step PDF instruction guide. You will need the following Public IP to access your test drive resources: 40.78.64.196 Connect to the FortiGate Web GUI on port 8443:
<https://40.78.64.196:8443>

Test Drive details

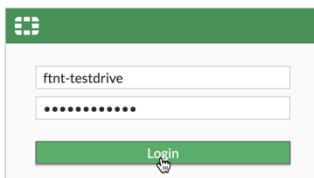
This test drive will allow you to experience how FortiGate-VM firewall enables enterprises to control their resources and applications in MS Azure through Fortinet solutions. Fortinet solutions provide the freedom to deploy any application on MS Azure without compromising security. You will configure a IPv4 policy on FortiGate-VM firewall GUI and enable different security profiles to provide secured access from your device to a web server hosted in MS Azure.

Documentation
[Test Drive User Manual](#)

2. Use the following credentials

username: ftnt-testdrive

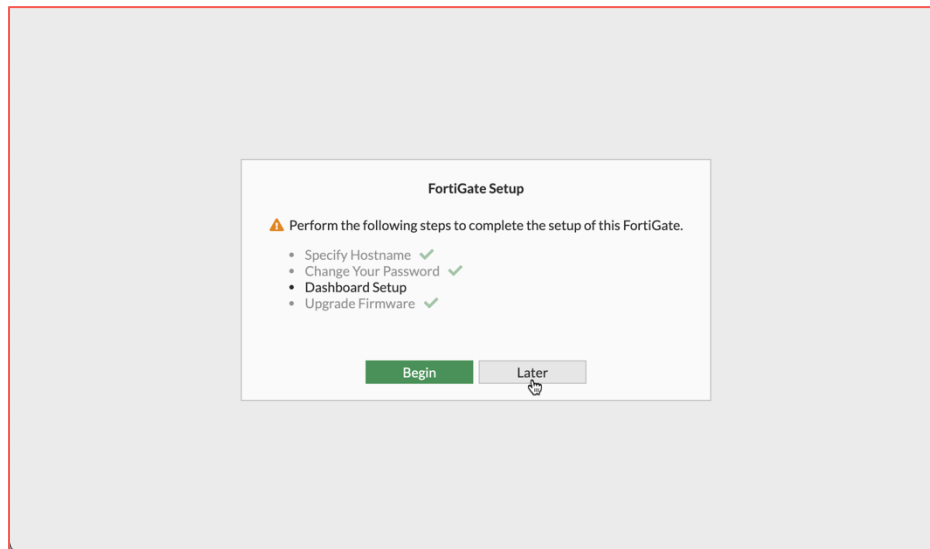
password: Fortinet@123



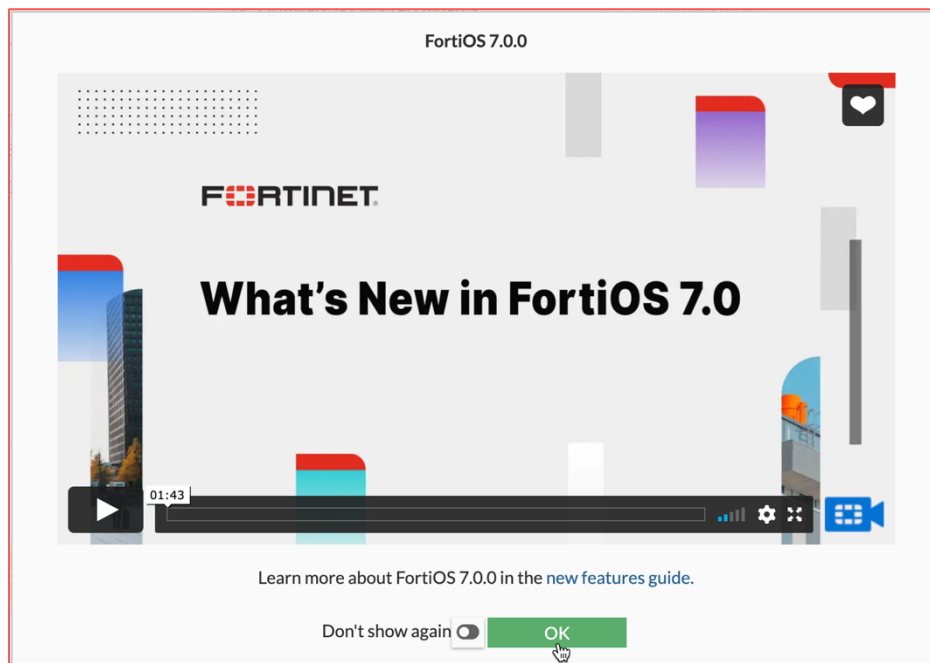
The image shows a login window for the FortiGate VM. It has a green header with the Fortinet logo. Below the header, there are two input fields: the first contains the username 'ftnt-testdrive' and the second contains a masked password represented by dots. At the bottom of the form is a green 'Login' button with a mouse cursor hovering over it.

Fortinet FortiGate – Azure Test Drive

3. **Click** the Later button to bypass FortiGate Dashboard setup



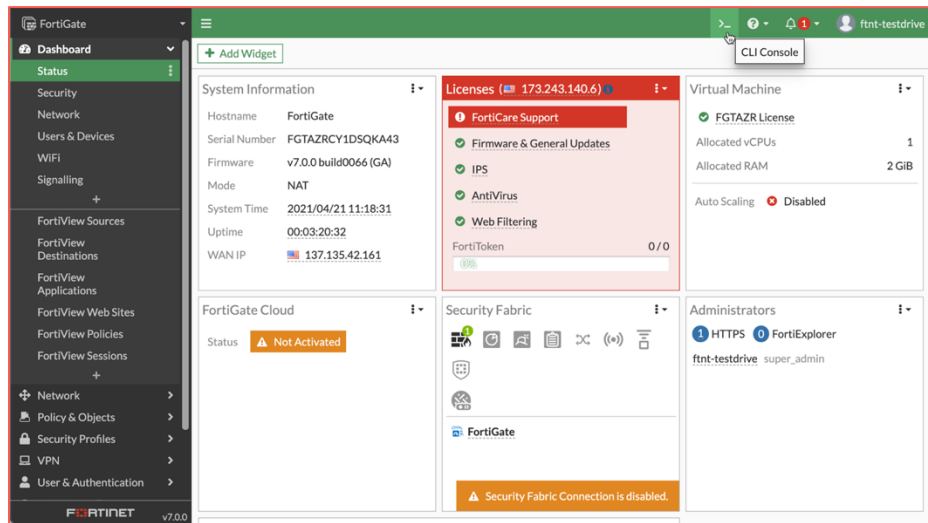
4. **Click** Ok to bypass "What's New in FortiOS 7.0"



Fortinet FortiGate – Azure Test Drive

5. Open the FortiGate CLI via the FortiGate GUI

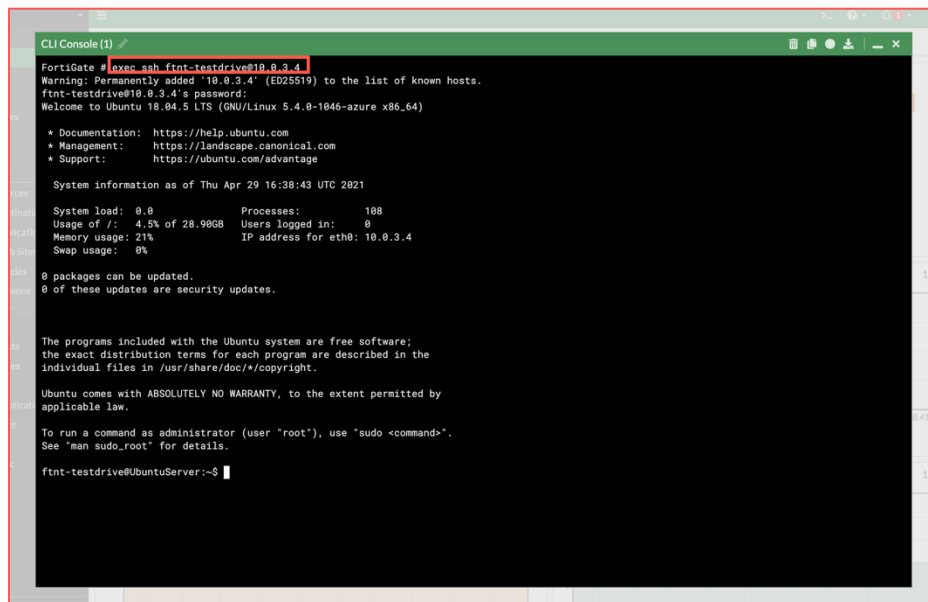
Click on the CLI Console Icon



6. Connect to the webserver host via the CLI Console

exec ssh ftnt-testdrive@10.0.3.4

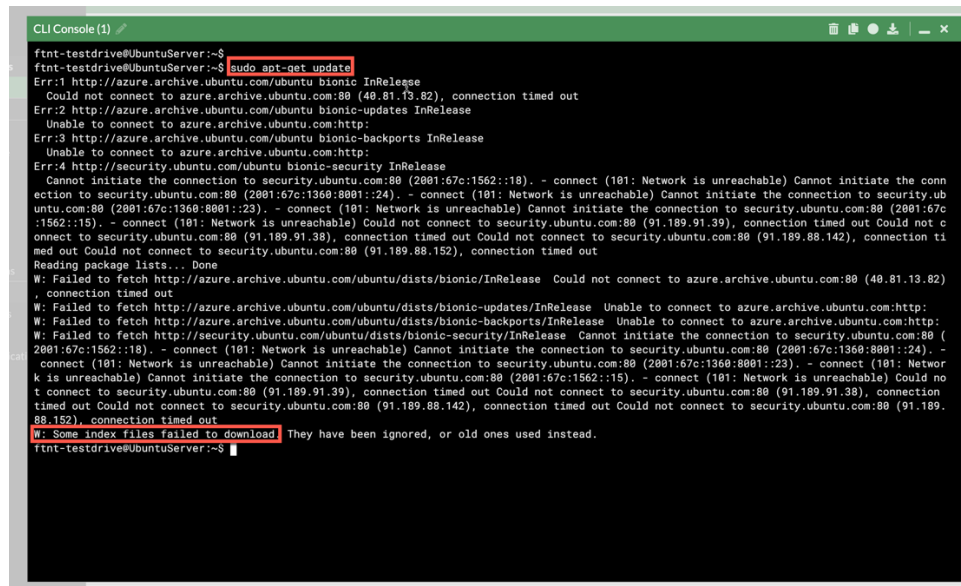
password: Fortinet@123



Fortinet FortiGate – Azure Test Drive

7. Attempt to update apt to install Apache2 webserver

```
sudo apt-get update
```



```
CLI Console (1)
ftnt-testdrive@UbuntuServer:~$ sudo apt-get update
Err:1 http://azure.archive.ubuntu.com/ubuntu bionic InRelease
  Could not connect to azure.archive.ubuntu.com:80 (40.81.13.82), connection timed out
Err:2 http://azure.archive.ubuntu.com/ubuntu bionic-updates InRelease
  Unable to connect to azure.archive.ubuntu.com:http:
Err:3 http://azure.archive.ubuntu.com/ubuntu bionic-backports InRelease
  Unable to connect to azure.archive.ubuntu.com:http:
Err:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
  Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1562::18). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1360:8001::24). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1360:8001::23). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1562::15). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (91.189.91.39), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.38), connection timed out Could not connect to security.ubuntu.com:80 (91.189.88.142), connection timed out Could not connect to security.ubuntu.com:80 (91.189.88.152), connection timed out
Reading package lists... Done
W: Failed to fetch http://azure.archive.ubuntu.com/ubuntu/dists/bionic/InRelease Could not connect to azure.archive.ubuntu.com:80 (40.81.13.82), connection timed out
W: Failed to fetch http://azure.archive.ubuntu.com/ubuntu/dists/bionic-updates/InRelease Unable to connect to azure.archive.ubuntu.com:http:
W: Failed to fetch http://azure.archive.ubuntu.com/ubuntu/dists/bionic-backports/InRelease Unable to connect to azure.archive.ubuntu.com:http:
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/bionic-security/InRelease Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1562::18). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1360:8001::24). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1360:8001::23). - connect (101: Network is unreachable) Cannot initiate the connection to security.ubuntu.com:80 (2001:67c:1562::15). - connect (101: Network is unreachable) Could not connect to security.ubuntu.com:80 (91.189.91.39), connection timed out Could not connect to security.ubuntu.com:80 (91.189.91.38), connection timed out Could not connect to security.ubuntu.com:80 (91.189.88.142), connection timed out Could not connect to security.ubuntu.com:80 (91.189.88.152), connection timed out
W: Some index files failed to download. They have been ignored, or old ones used instead.
ftnt-testdrive@UbuntuServer:~$
```

The webserver host cannot connect to the Internet and will stall attempting to update the apt package repositories.

This is because an Azure route table with a User Defined Route has been added to the VNET to force the webserver host's outbound communication through the FortiGate, and the FortiGate does not have a policy to allow internet connectivity.

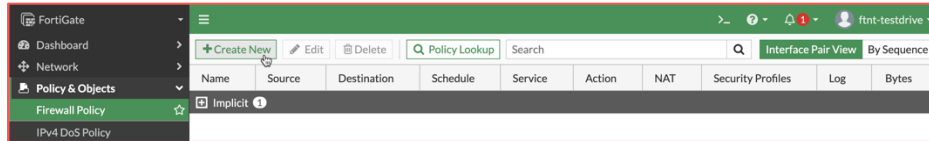
8. Minimize the CLI Console.



TASK 2 – ADD OUTBOUND CONNECTIVITY POLICY

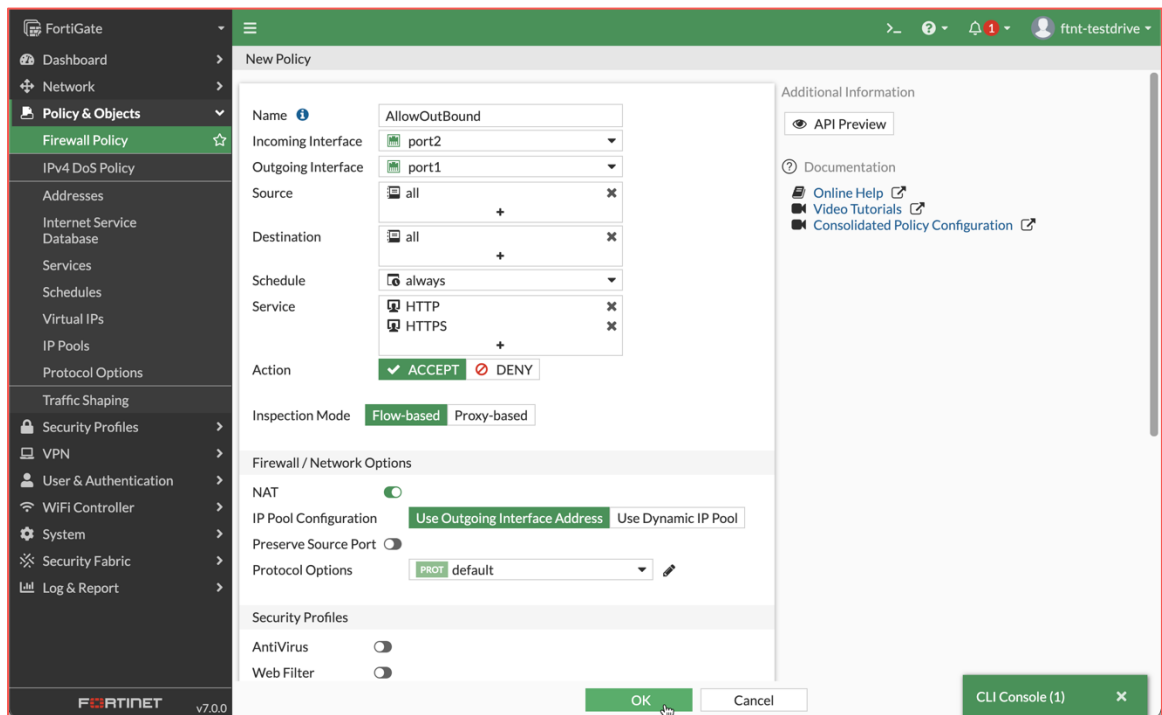
1. **Select** "Policy & Objects" -> "Firewall Policy"
2. **Click** the "+ Create New" button

Fortinet FortiGate – Azure Test Drive



3. Configure the Policy

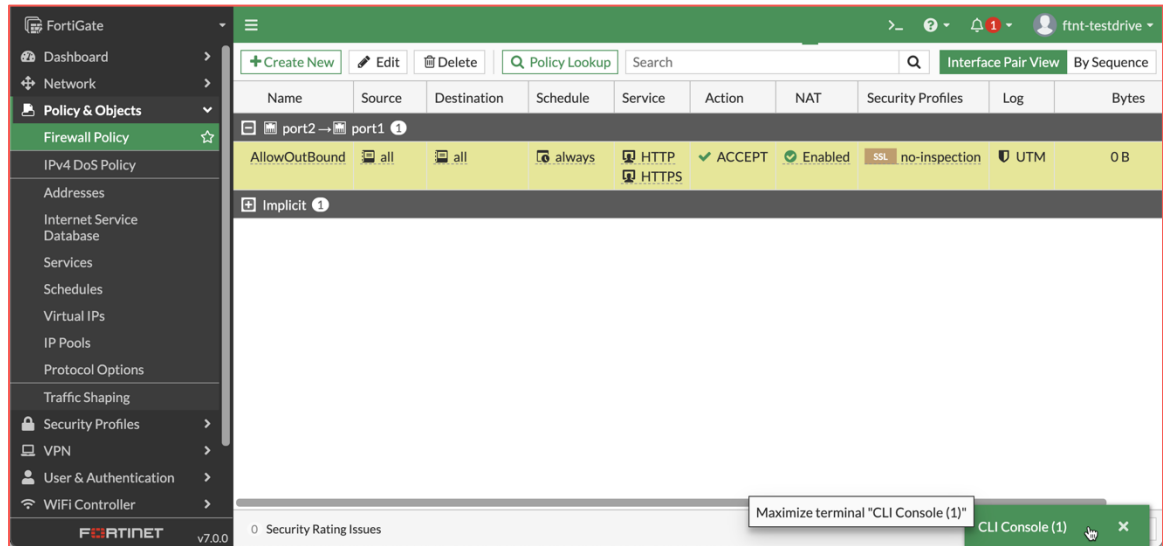
- **Name:** AllowOutBound
- **Incoming Interface:** port2
- **Outgoing Interface:** port1
- **Source:** all
- **Destination:** all
- **Schedule:** always
- **Service:** HTTP & HTTPS
- **Enable:** NAT
- **Click OK**



Fortinet FortiGate – Azure Test Drive

TASK 3 – INSTALL APACHE2 WEBSERVER

1. Maximize the CLI Console session



2. Attempt to install the Apache2 webserver

```
sudo apt-get update  
sudo apt-get install apache2 -y
```

This time apt-get should update and the Webserver should install successfully, because the outbound traffic was **allowed** to pass through the FortiGate.

3. Close the CLI Console

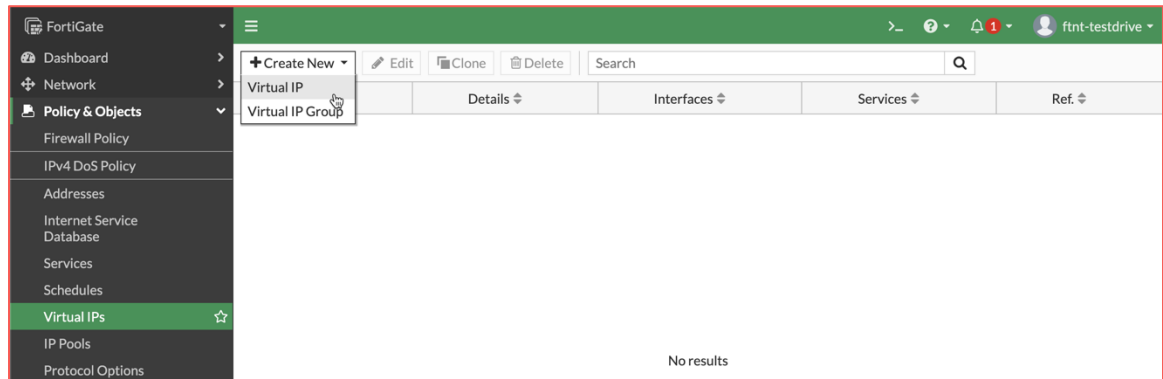
TASK 4 – CONFIGURE FORTIGATE FOR WEB TRAFFIC

1. In a new tab in your web browser, attempt to connect via http to the same public IP as the FortiGate.

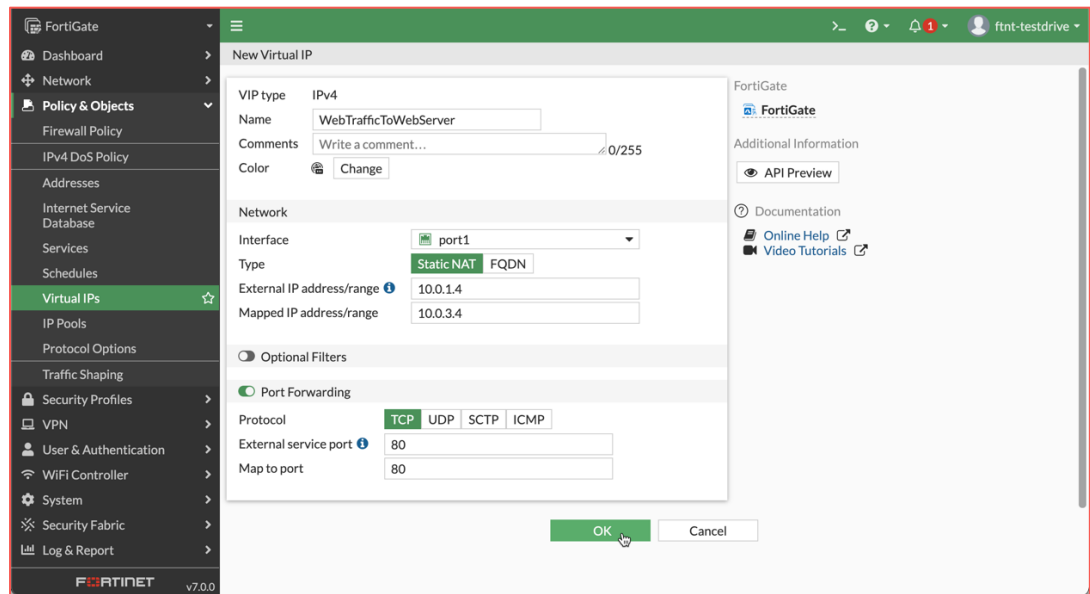
Fortinet FortiGate – Azure Test Drive

This will not be successful because the FortiGate is not configured to respond to port 80.

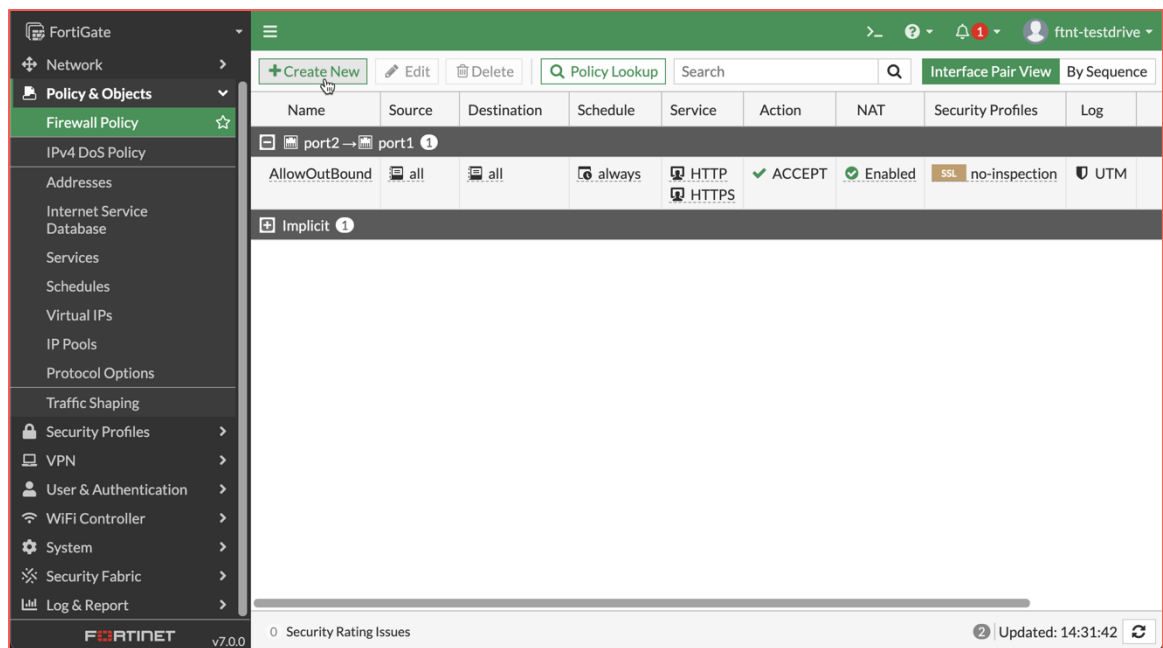
2. In the FortiGate GUI select "Policy & Objects" -> "Virtual IPs"
3. **Click** the "+ Create New" button and select "Virtual IP"



4. Create a new virtual IP to forward traffic for interface "port1"
 - **Name:** WebTrafficToWebserver
 - **Interface:** port1
 - **External IP Address/Range:** 10.0.1.4
 - **Mapped IP Address/Range:** 10.0.3.4
 - **Enable** Port Forwarding
 - **External Service Port:** 80
 - **Map to Port:** 80
 - **Click** OK



5. **Select** "Policy & Objects" -> "Firewall Policy" You should see the AllowOutBound policy that was previously created.

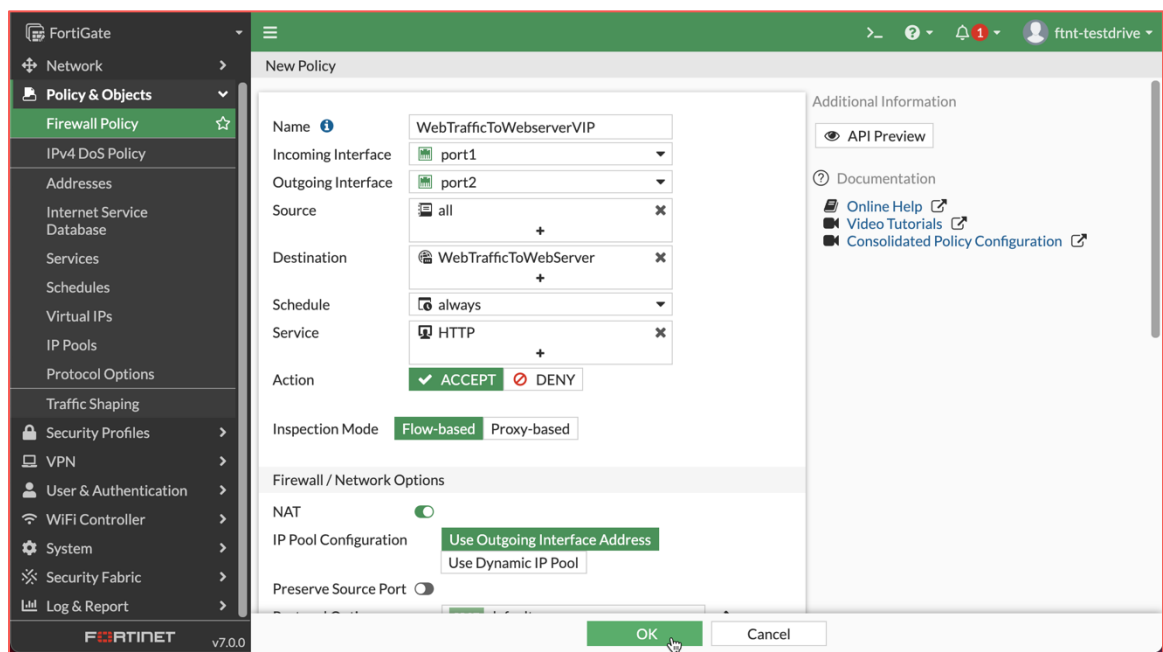


6. **Click** the "+ Create New" button.

Fortinet FortiGate – Azure Test Drive

7. The new policy will allow all traffic in port1 and out port2 (the reverse of the previous policy).

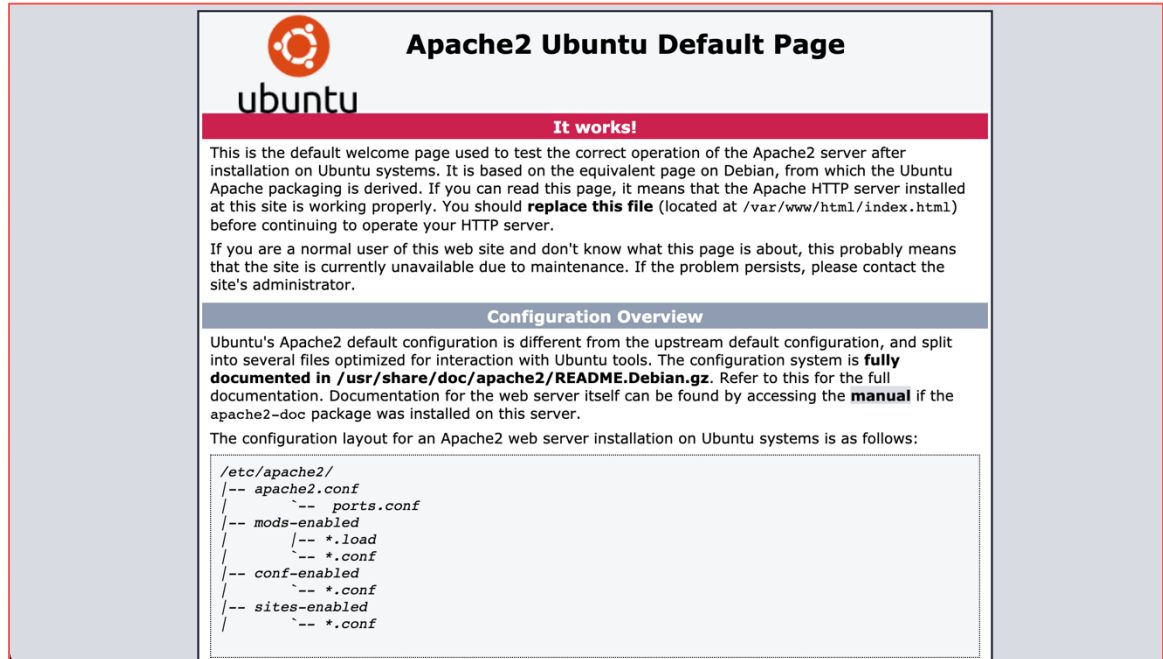
- **Name:** WebTrafficToWebserverVIP
- **Incoming Interface:** port1
- **Outgoing Interface:** port2
- **Source:** all
- **Destination:** WebTrafficToWebserver
- **Service:** HTTP
- **Click OK**



TASK 5 – CONNECT TO WEBSERVER

1. Attempt to connect again to the public IP via http. This time you should see the default Apache2 for Ubuntu web page.

Fortinet FortiGate – Azure Test Drive



2. Success!

This Azure FortiGate Test Drive is a simple use case that enables hosts in a protected subnet the ability to access the Internet via the FortiGate and allow external clients access to resources in a protected subnet via the FortiGate.

Whether the traffic is outbound or inbound it can be monitored and managed by the FortiGate allowing for secured network communications.

Fortinet FortiGate – Azure Test Drive