Fortigate

Microsoft Azure Test Drive

A picture containing chart

Description automatically generated

Test Drive Guide

Updated: December 15th, 2021

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

Diagram

Description automatically generated

## TASK 1 – Connect to FortiGate & Webserver

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

Graphical user interface, text, application, email

Description automatically generated

1. Use the following credentials

**username**: ftnt-testdrive  
**password**: Fortinet@123

Graphical user interface

Description automatically generated

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

Graphical user interface, application

Description automatically generated

1. **Click** Ok to bypass “What’s New in FortiOS 7.0”

Graphical user interface, text, application

Description automatically generated

1. Open the FortiGate CLI via the FortiGate GUI

***Click*** on the CLI Console Icon

Graphical user interface, application, website

Description automatically generated

1. Connect to the webserver host via the CLI Console

**exec ssh ftnt-testdrive@10.0.3.4**  
**password**: Fortinet@123

Text

Description automatically generated

1. Attempt to update apt to install Apache2 webserver

**sudo apt-get update**

**Text

Description automatically generated**

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.

1. Minimize the CLI Console.

Text

Description automatically generated

## TASK 2 – Add outbound connectivity Policy

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

Graphical user interface, application

Description automatically generated

1. Configure the Policy
   * **Name**: AllowOutBound
   * **Incoming Interface**: port2
   * **Outgoing Interface**: port1
   * **Source**: all
   * **Destination**: all
   * **Schedule**: always
   * **Service**: HTTP & HTTPS
   * **Enable:** NAT
   * **Click** OK

Graphical user interface, application

Description automatically generated

## TASK 3 – Install Apache2 Webserver

1. Maximize the CLI Console session

Graphical user interface, text, application

Description automatically generated

1. 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.

1. 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.

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

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

Graphical user interface, text, application, email

Description automatically generated

1. 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

Graphical user interface, application

Description automatically generated

1. **Select** “Policy & Objects” -> “Firewall Policy” You should see the AllowOutBound policy that was previously created.

Graphical user interface, text, application

Description automatically generated

1. **Click** the “+ Create New” button.
2. 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

Graphical user interface, application

Description automatically generated

## 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.

Graphical user interface, text, email

Description automatically generated

1. 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.