**FORTIWEB**

**Microsoft Azure Test Drive**

A picture containing chart

Description automatically generated

**Test Drive Guide**

**March 18th, 2022**

# 

# Fortinet FortiWeb – Azure Test Drive



**TABLE OF**

**CONTENTS**

[Fortinet FortiWeb – Azure Test Drive 1](#_Toc98511539)

[TASK 1 – CONNECT TO FORTIWEB & WEBSERVER 6](#_Toc98511540)

[1. When the Test Drive is ready *click* on the FortiWeb link to open the GUI. 6](#_Toc98511541)

[2. Use the following credentials 6](#_Toc98511542)

[3. Once you *login* you willbe at the FortiWeb Dashboard setup 7](#_Toc98511543)

[TASK 2 – CHECK CONNECTIVITY TO WEB SERVER 7](#_Toc98511544)

[1. Click on CLI Console to check the connectivity to the web server 7](#_Toc98511545)

[4. Check connectivity to the web server via CLI-Console 8](#_Toc98511546)

[TASK 3 – CREATE SERVER POOL 9](#_Toc98511547)

[1. Navigate to Server Objects >> Server >> Server Pool >> Create new 9](#_Toc98511548)

[2. Input information as shown below. Select the Server Balance option for Server Health check option to appear. Click OK. 9](#_Toc98511549)

[3. Once click OK in the above step the greyed out Create new button should now appear to create the Server object. 10](#_Toc98511550)

[TASK 4 – CREATE VIRTUAL SERVER AND IP 11](#_Toc98511551)

[TASK 5 – CREATE WEB PROTECTION PROFILE 14](#_Toc98511552)

[TASK 7 – PERFORM AN ATTACK 15](#_Toc98511553)

[TASK 8 – PROTECT WEB SERVER FROM ATTACK 16](#_Toc98511554)

**Fortinet FortiWeb – Azure Test Drive**

**FORTIWEB**

**TEST DRIVE**

This test drive will allow you to experience how a FortiWeb Web Application firewall enables enterprises to protect their web 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 Server objects, Virtual servers, and Server policies on the FortiWeb-VM via the FortiWeb GUI to install and enable a webserver hosted in Azure access to the Internet and then enable Virtual IPs to protect the web servers against OWASP Top 10 and other web attacks.

**Fortinet FortiGate – Azure Test Drive** page3image45932048

Diagram

Description automatically generated

**Fortinet FortiWeb – Azure Test Drive** page3image45932048

# TASK 1 – CONNECT TO FORTIWEB & WEBSERVER

## Access the Test Drive Components.

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

Graphical user interface, text, application, Word, email

Description automatically generated

1. Use the following credentials

**username**: ftnt-testdrive

**password**: Fortinet@123

Graphical user interface

Description automatically generated

**Fortinet FortiGate – Azure Test Drive** page3image45932048

1. Upon ***login*** the FortiWeb Dashboard setup is displayed

Graphical user interface, application

Description automatically generated

# TASK 2 – CHECK CONNECTIVITY TO WEB SERVER

## Verify Web Server Connectivity

1. Click on CLI Console to check the connectivity to the web server

Graphical user interface, text, application

Description automatically generated

**Fortinet FortiWeb – Azure Test Drive** page3image45932048

1. Check connectivity to the web server via CLI-Console

**execute ping 10.0.3.4**

Graphical user interface, text, application

Description automatically generated

# TASK 3 – CREATE SERVER POOL

## Create Server Pool for Web Server

1. Navigate to Server Objects >> Server >> Server Pool >> Create new

Graphical user interface, application

Description automatically generated

1. Input information as shown below. Select the Server Balance option for Server Health check option to appear. Click OK.

Graphical user interface, application

Description automatically generated

1. Once click OK in the above step the greyed out Create new button should now appear to create the Server object.

Click “Create New”

Graphical user interface, text, application

Description automatically generated

1. Now enter the IP address of your application server in this case it is the IP address of Apache Server, the port number the pool member/application server listens for connections.

Click OK once you enter the information.

Graphical user interface, application

Description automatically generated

# TASK 4 – CREATE VIRTUAL SERVER AND IP

## Create Virtual Server and IP

1. Now we will need to create the Virtual Server IP on which the Traffic destined for server pool member arrives. When FortiWeb receives traffic destined for a Virtual server it can then forward to its pool members.

Graphical user interface, application, Word

Description automatically generated

1. Enter the name for the Virtual Server and click OK

Graphical user interface, application

Description automatically generated

1. Click Create new as shown below to now create Virtual server item.

Graphical user interface, text, application

Description automatically generated

1. Virtual Server item can be an IP address of the interface or an IP other than the interface. In this case we will use the interface IP - Turn on the Radio button for “use interafce IP”, a drop down with interfaces will appear. Select Port1 as the interface for this Virtual Server item and click OK.

Graphical user interface, application

Description automatically generated

1. The Virtual Server for the Apache Server is now using the IP address of the Port1 Interface.

Graphical user interface, application

Description automatically generated

# TASK 5 – CREATE WEB PROTECTION PROFILE

Create Web Protection Profile

1. We will now create a Policy to apply a protection profile to protect our application Server. Before creating a policy let’s look at few default protection profiles that FortiWeb is configured with. The Inline Standard protection profile consists of signatures to protect against SQL injection, XSS and other generic attacks.

Navigate to Policy >> Web Protection Profile

Graphical user interface, table

Description automatically generated

NOTE: You can create your custom Protection profile as well.

1. Now let’s create a Server policy. Input Name for the server policy, Select the Virtual Server, Server pool which we created in the earlier steps from the drop down and finally Select the HTTP service. In this step we are not attaching the Protection profile. Click OK

Graphical user interface, application

Description automatically generated

# TASK 7 – PERFORM AN ATTACK

## Perform an Attack

1. Now let’s Navigate to the browser and type the Public IP assigned to your FortiWeb instance to get to the web browser. <http://FortiWebIP>

Graphical user interface, text, application

Description automatically generated

1. Let’s perform a SQLi attack. To perform a SQLi attack append **?name=' OR 'x'='x** to your URL.

For example: http://52.190.192.174/?name=' OR 'x'='x

The attack **will** go through.

Graphical user interface, text, application

Description automatically generated

# TASK 8 – PROTECT WEB SERVER FROM ATTACK

## Protect the Web Server

1. We will now attach the FortiWeb protection profile.

Click the dropdown and attack inline standard protection. Click OK.

**Graphical user interface, application

Description automatically generated**

1. Repeat the same step to perform SQLi attack in the browser.

http://52.190.192.174/?name=' OR 'x'='x

You will see that FortiWeb now blocks the SQLi attack.

Graphical user interface, text, application

Description automatically generated