

FORTIWEB

Microsoft Azure Test Drive



Test Drive Guide
March 18th, 2022

Fortinet FortiWeb – Azure Test Drive

© Fortinet Inc. All Rights Reserved.

TABLE OF CONTENTS

FORTINET FORTIWEB – AZURE TEST DRIVE.....	1
TASK 1 – CONNECT TO FORTIWEB & WEBSERVER.....	6
1. WHEN THE TEST DRIVE IS READY <i>CLICK</i> ON THE FORTIWEB LINK TO OPEN THE GUI.....	6
2. USE THE FOLLOWING CREDENTIALS.....	6
3. ONCE YOU <i>LOGIN</i> YOU WILL BE AT THE FORTIWEB DASHBOARD SETUP.....	6
TASK 2 – CHECK CONNECTIVITY TO WEB SERVER.....	7
1. CLICK ON CLI CONSOLE TO CHECK THE CONNECTIVITY TO THE WEB SERVER	7
4. CHECK CONNECTIVITY TO THE WEB SERVER VIA CLI-CONSOLE	8
TASK 3 – CREATE SERVER POOL	8
1. NAVIGATE TO SERVER OBJECTS >> SERVER >> SERVER POOL >> CREATE NEW	8
2. INPUT INFORMATION AS SHOWN BELOW. SELECT THE SERVER BALANCE OPTION FOR SERVER HEALTH CHECK OPTION TO APPEAR. CLICK OK.....	9
3. ONCE CLICK OK IN THE ABOVE STEP THE GREYED OUT CREATE NEW BUTTON SHOULD NOW APPEAR TO CREATE THE SERVER OBJECT.	9
TASK 4 – CREATE VIRTUAL SERVER AND IP	11
TASK 5 – CREATE WEB PROTECTION PROFILE	14
TASK 7 – PERFORM AN ATTACK	15
TASK 8 – PROTECT WEB SERVER FROM ATTACK	16

Fortinet FortiWeb – Azure Test Drive

© Fortinet Inc. All Rights Reserved.

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.

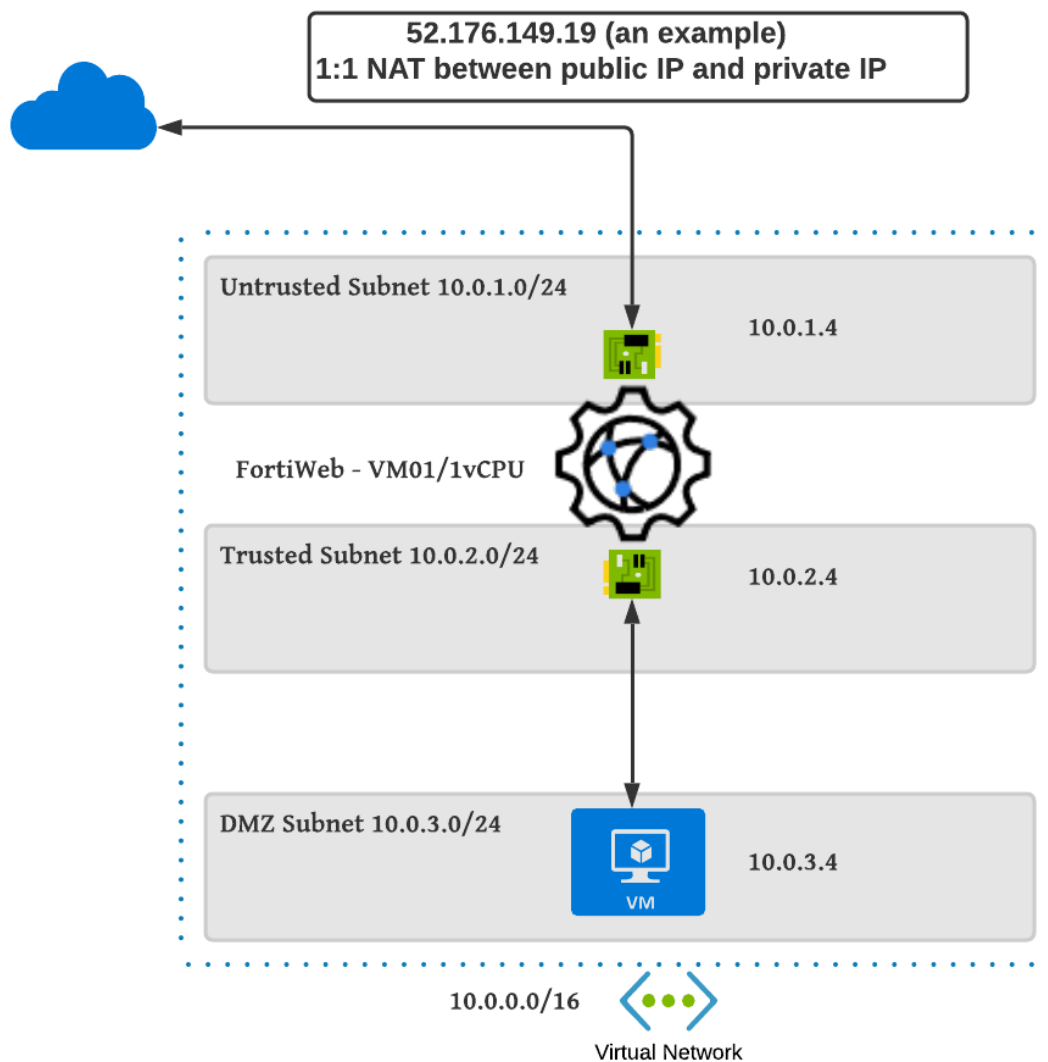
ABOUT THE TEST DRIVE ENVIRONMENT

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

© Fortinet Inc. All Rights Reserved.

FortiWeb Azure Test Drive

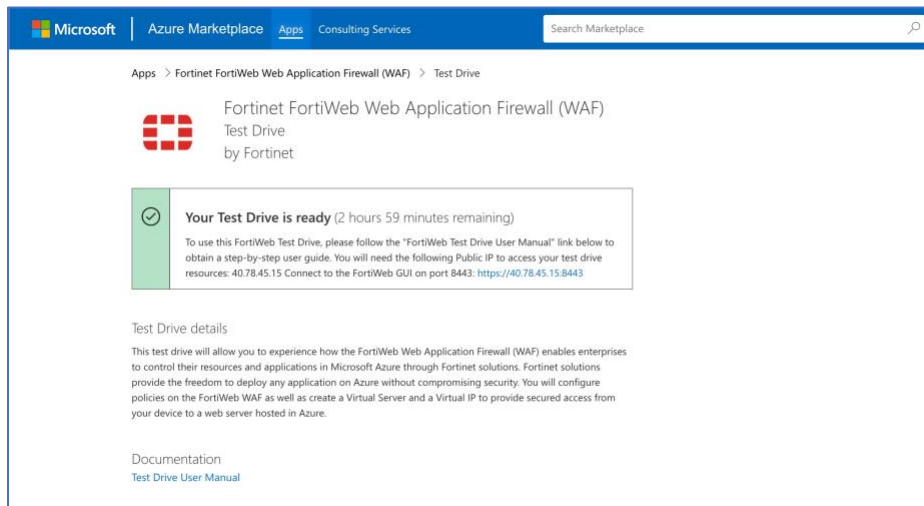


Fortinet FortiWeb – Azure Test Drive

TASK 1 – CONNECT TO FORTIWEB & WEBSERVER

Access the Test Drive Components.

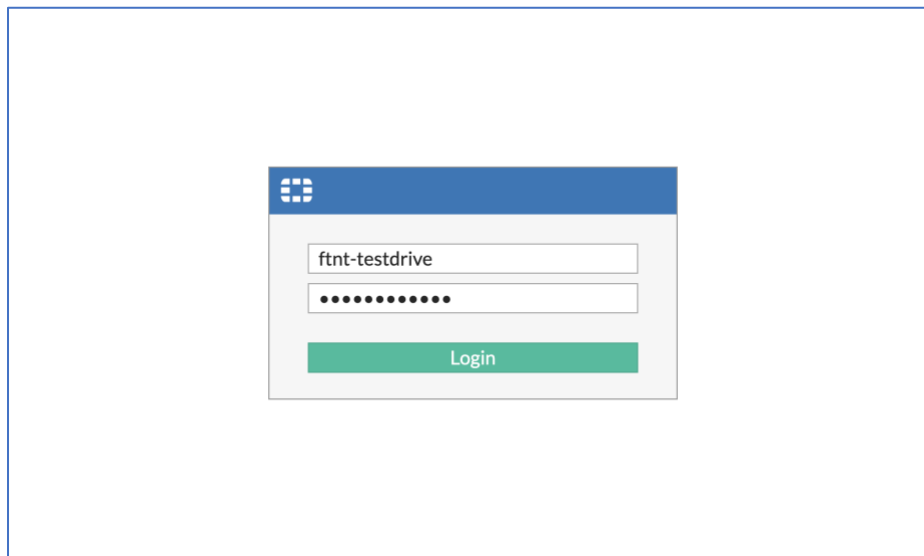
1. When the Test Drive is ready **click** on the FortiWeb link to open the GUI.



2. Use the following credentials

username: ftnt-testdrive

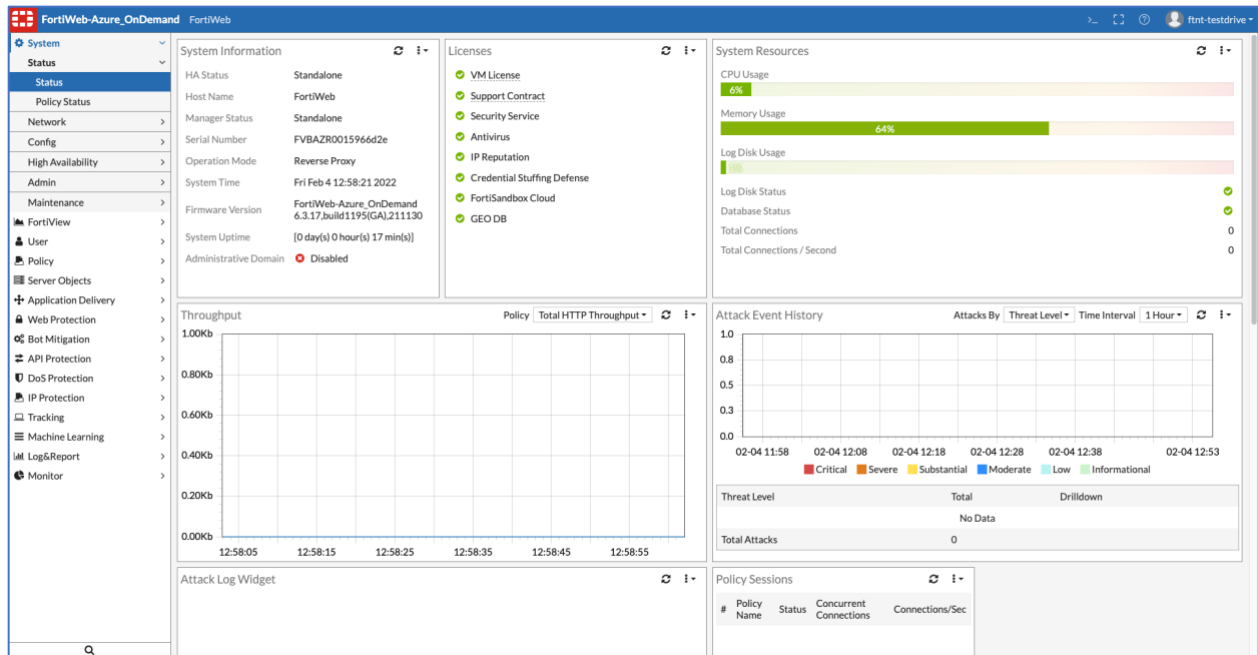
password: Fortinet@123



Fortinet FortiGate – Azure Test Drive

© Fortinet Inc. All Rights Reserved.

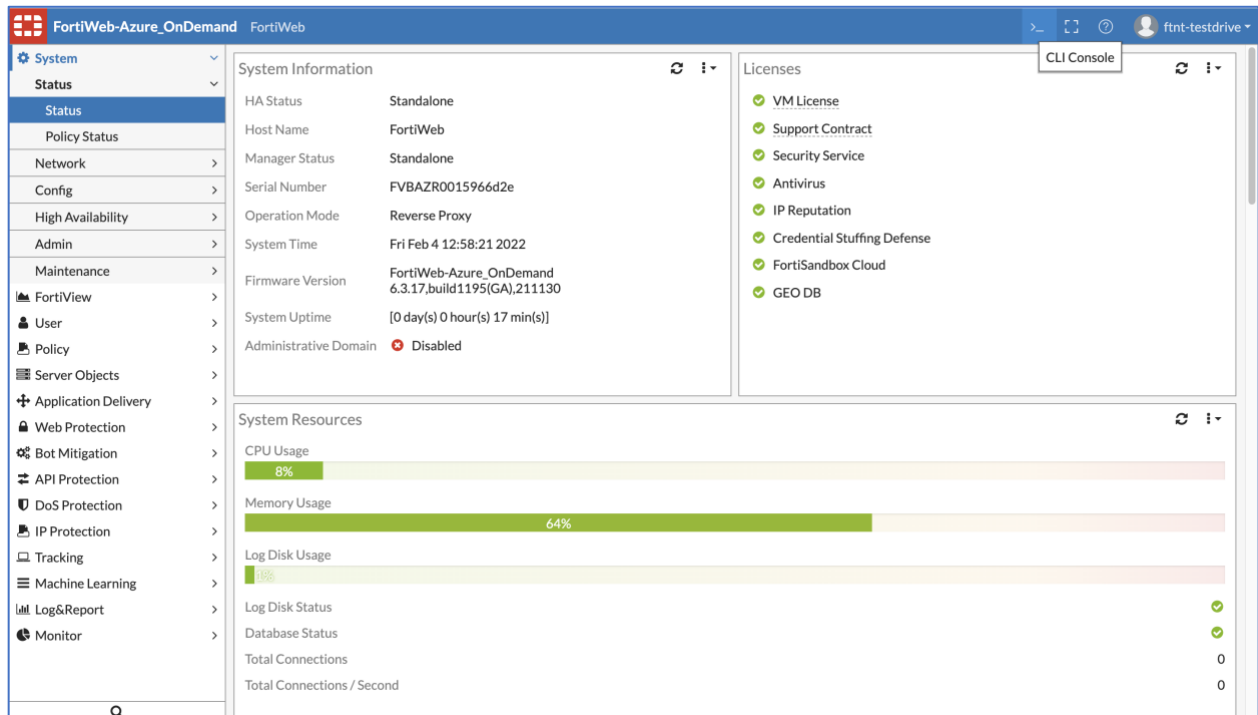
3. Upon **login** the FortiWeb Dashboard setup is displayed



TASK 2 – CHECK CONNECTIVITY TO WEB SERVER

Verify Web Server Connectivity

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

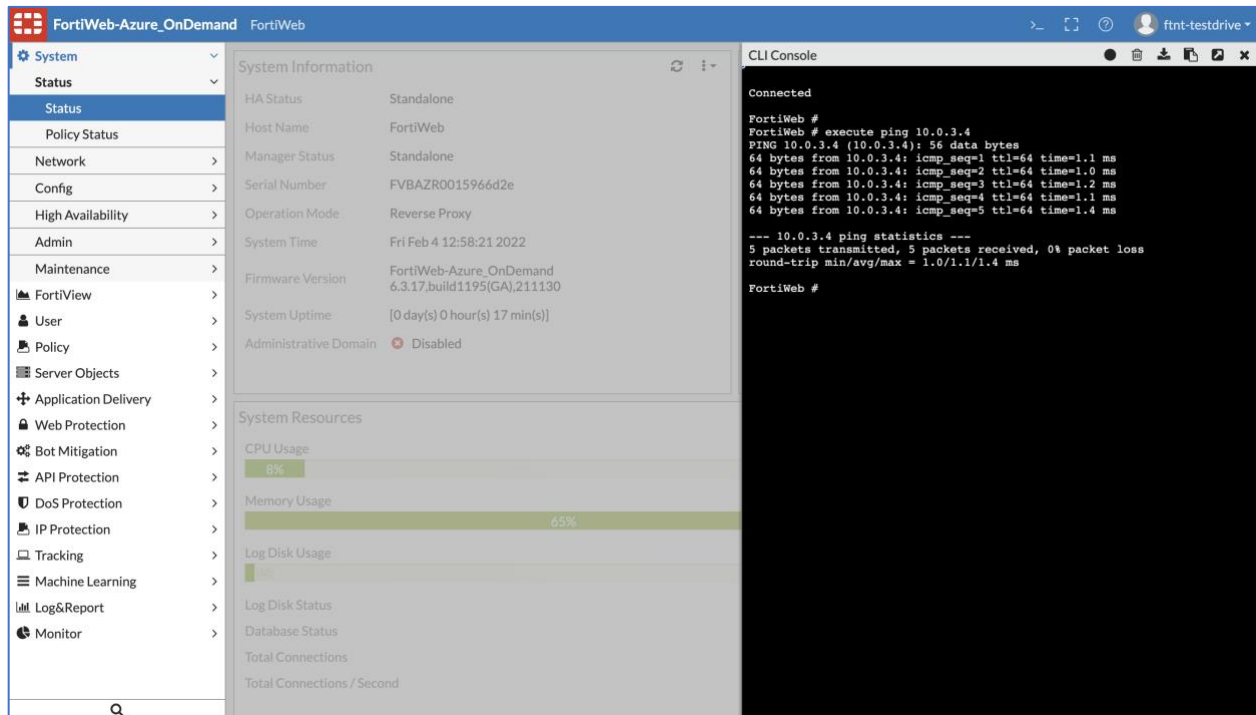


Fortinet FortiWeb – Azure Test Drive

© Fortinet Inc. All Rights Reserved.

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

execute ping 10.0.3.4



The screenshot displays the FortiWeb management interface. On the left is a navigation menu with categories like System, Status, Policy Status, Network, Config, High Availability, Admin, Maintenance, FortiView, User, Policy, Server Objects, Application Delivery, Web Protection, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Machine Learning, Log&Report, and Monitor. The main panel is divided into 'System Information' and 'System Resources'. The 'System Information' section shows details such as HA Status (Standalone), Host Name (FortiWeb), Manager Status (Standalone), Serial Number (FVBAZR0015966d2e), Operation Mode (Reverse Proxy), System Time (Fri Feb 4 12:58:21 2022), Firmware Version (FortiWeb-Azure_OnDemand 6.3.17.build1195(GA),211130), System Uptime ([0 day(s) 0 hour(s) 17 min(s)]), and Administrative Domain (Disabled). The 'System Resources' section shows CPU Usage at 8%, Memory Usage at 65%, and Log Disk Usage at 0%. On the right, the 'CLI Console' window shows the command 'execute ping 10.0.3.4' being executed, resulting in five successful ping responses with varying times (1.1 ms to 1.4 ms) and 0% packet loss.

```
FortiWeb # execute ping 10.0.3.4
PING 10.0.3.4 (10.0.3.4): 56 data bytes
64 bytes from 10.0.3.4: icmp_seq=1 ttl=64 time=1.1 ms
64 bytes from 10.0.3.4: icmp_seq=2 ttl=64 time=1.0 ms
64 bytes from 10.0.3.4: icmp_seq=3 ttl=64 time=1.2 ms
64 bytes from 10.0.3.4: icmp_seq=4 ttl=64 time=1.1 ms
64 bytes from 10.0.3.4: icmp_seq=5 ttl=64 time=1.4 ms

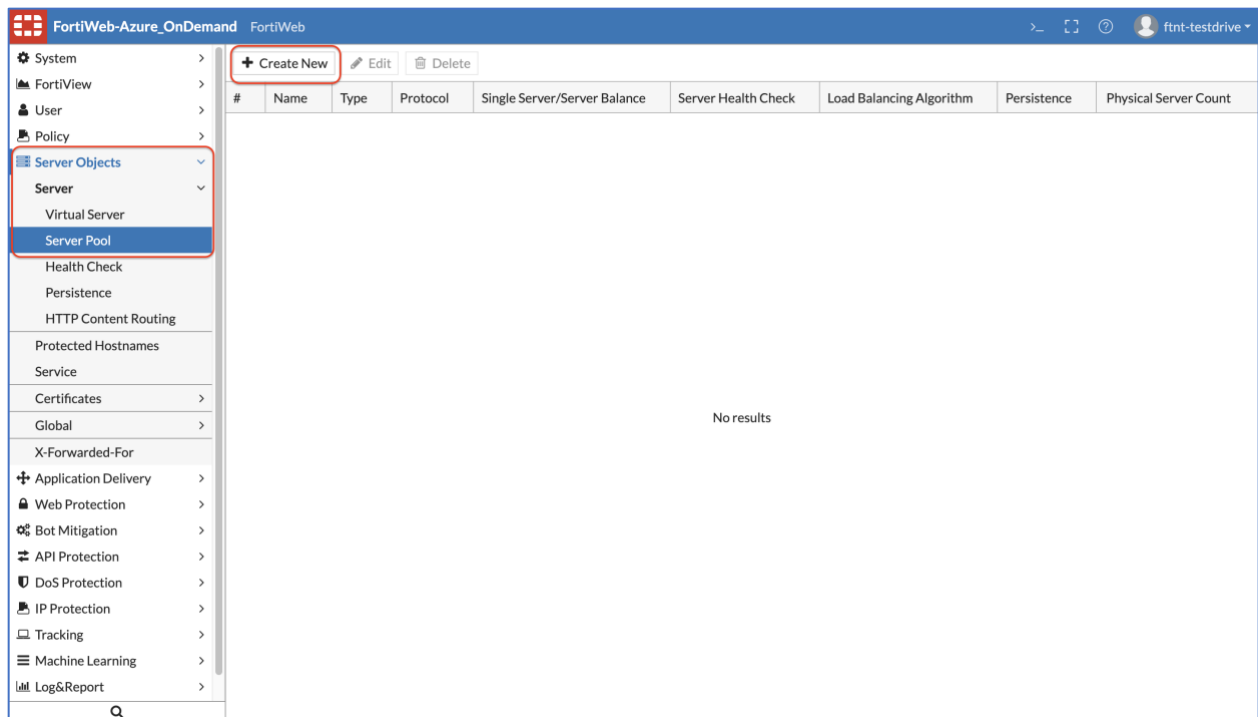
--- 10.0.3.4 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.1/1.4 ms

FortiWeb #
```

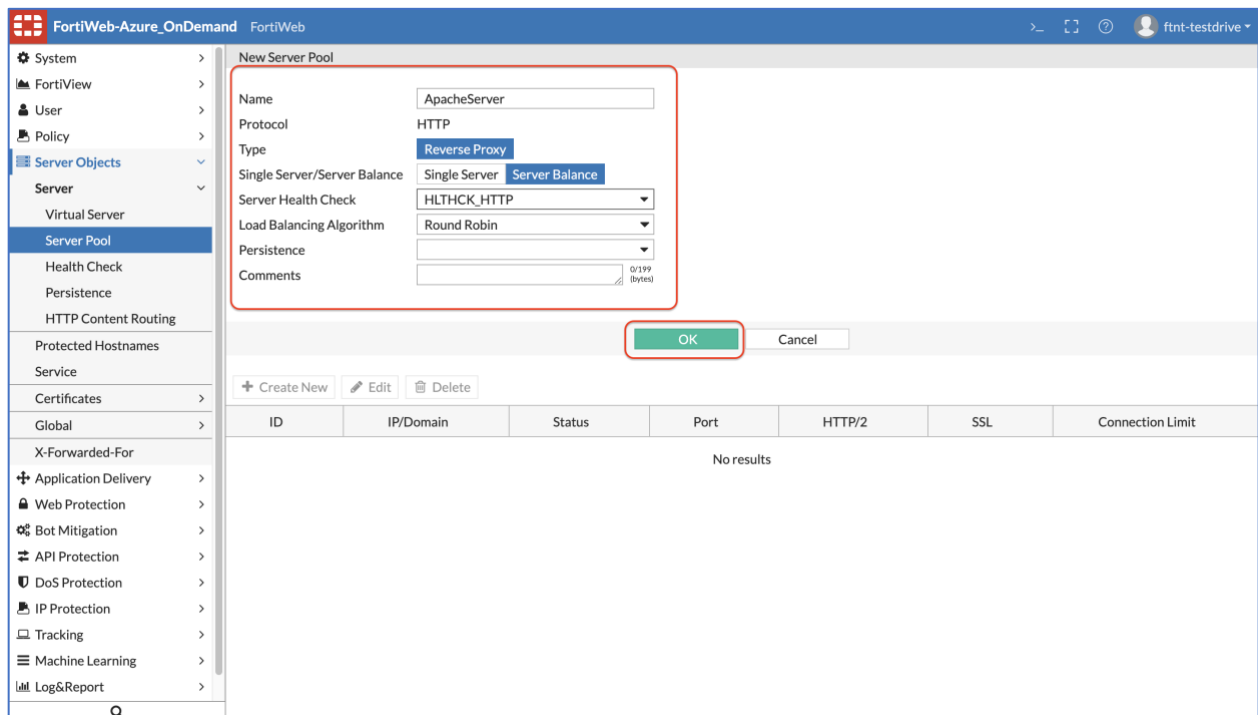
TASK 3 – CREATE SERVER POOL

Create Server Pool for Web Server

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

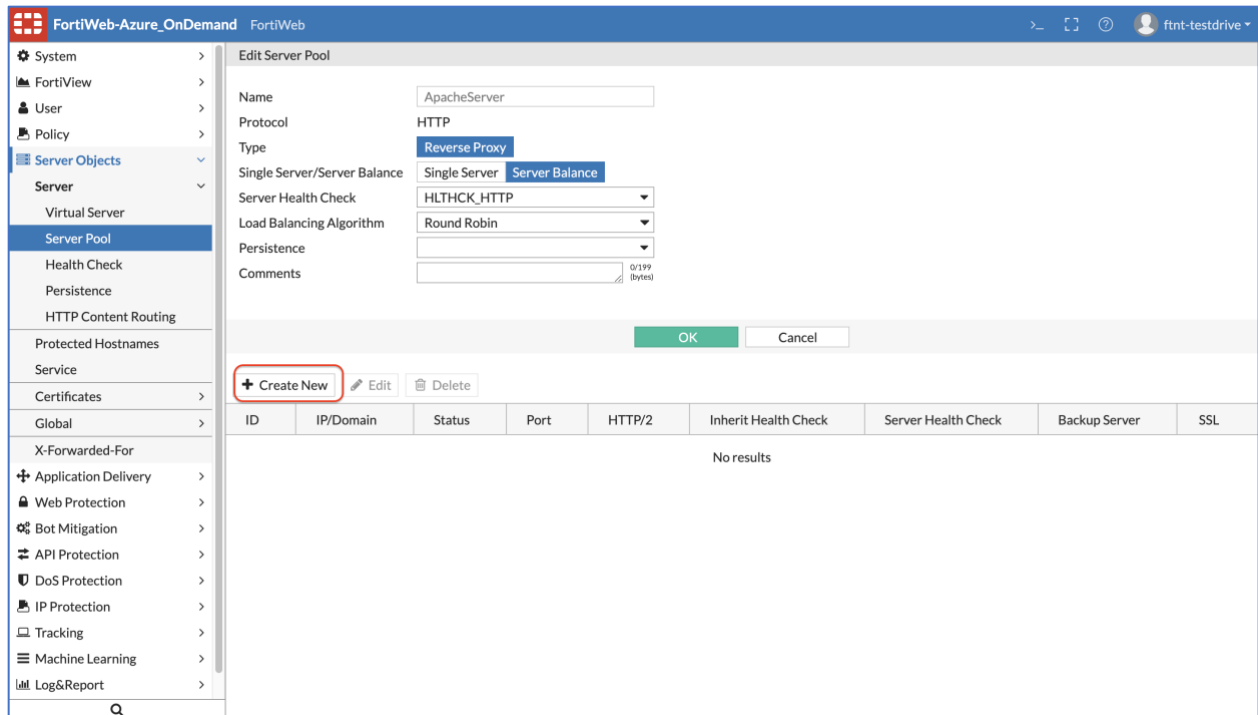


2. Input information as shown below. Select the Server Balance option for Server Health check option to appear. Click OK.



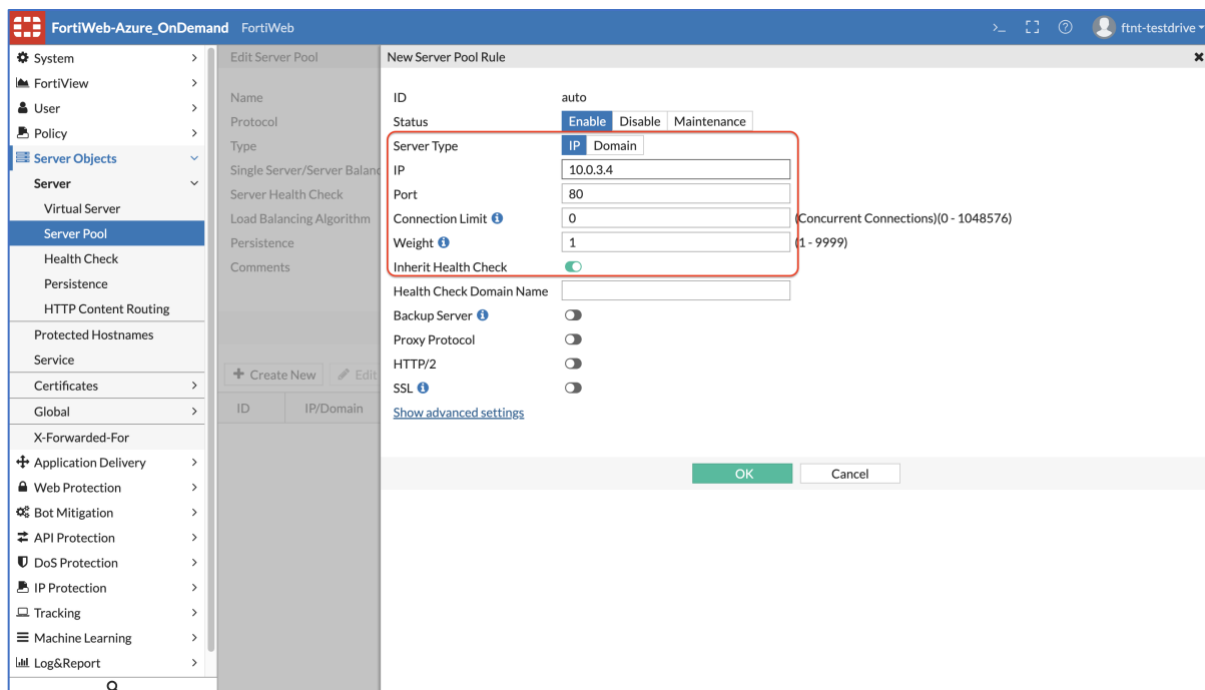
3. Once click OK in the above step the greyed out Create new button should now appear to create the Server object.

Click "Create New"



- 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.

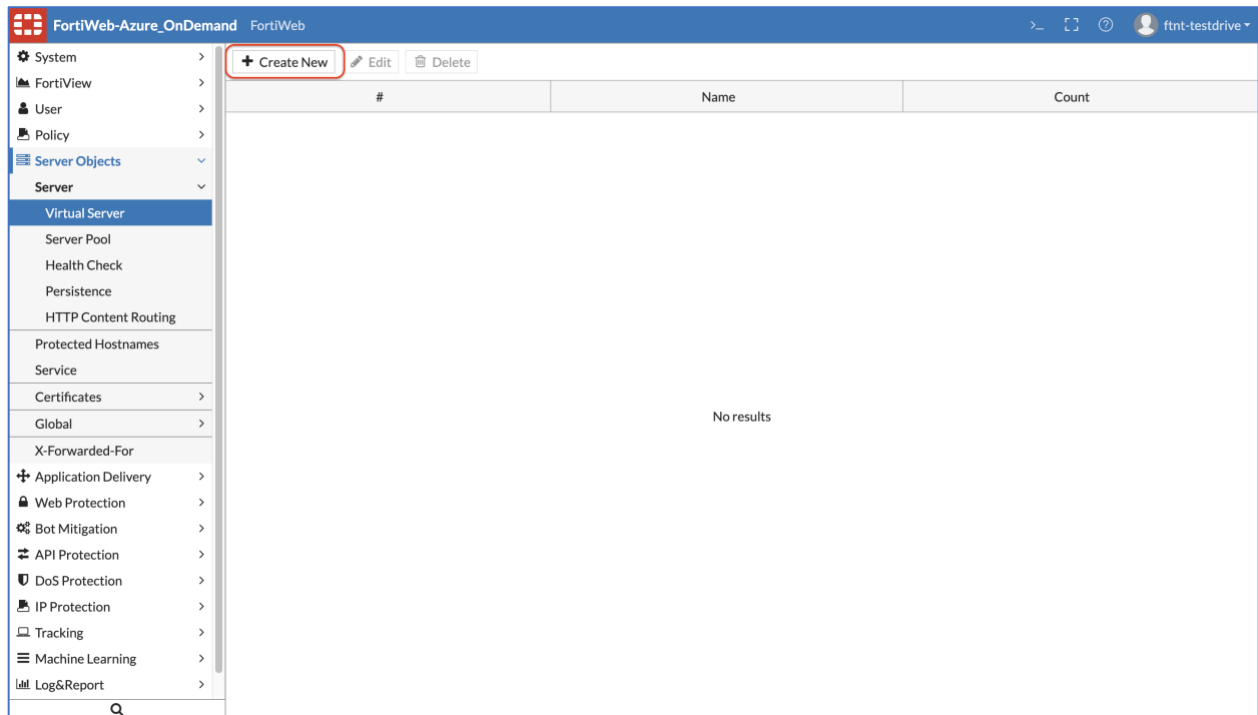
Click OK once you enter the information.



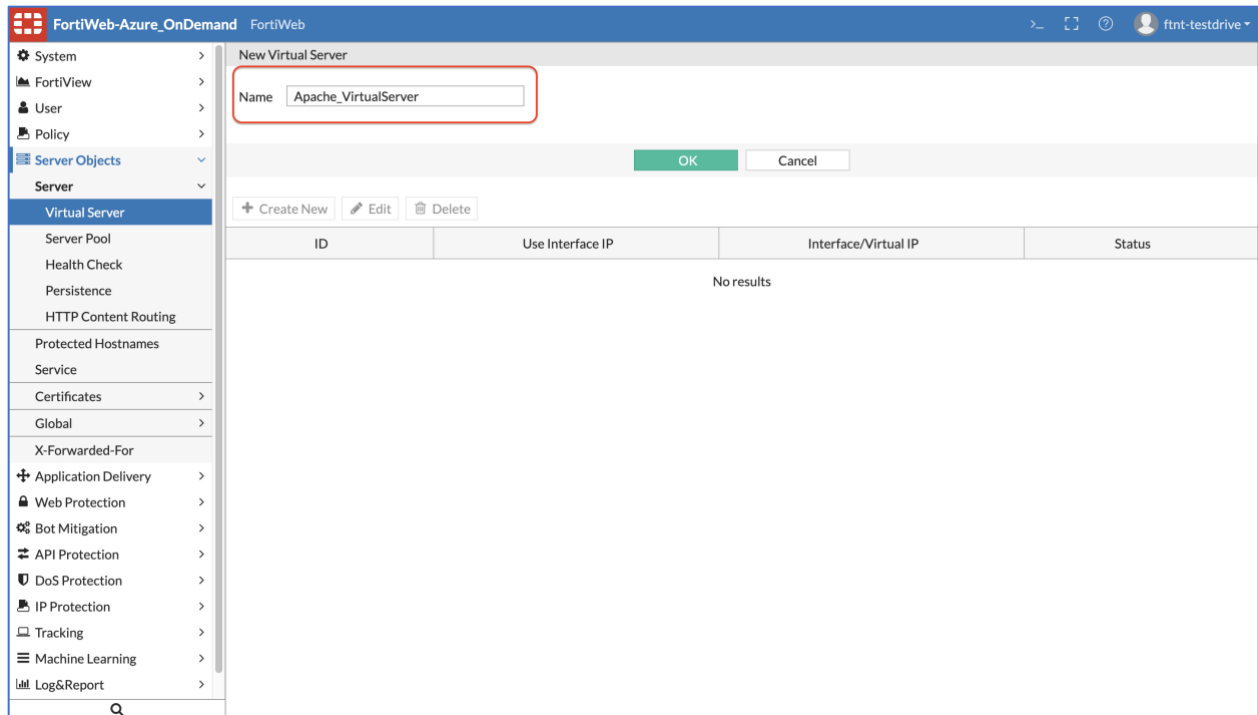
TASK 4 – CREATE VIRTUAL SERVER AND IP

Create Virtual Server and IP

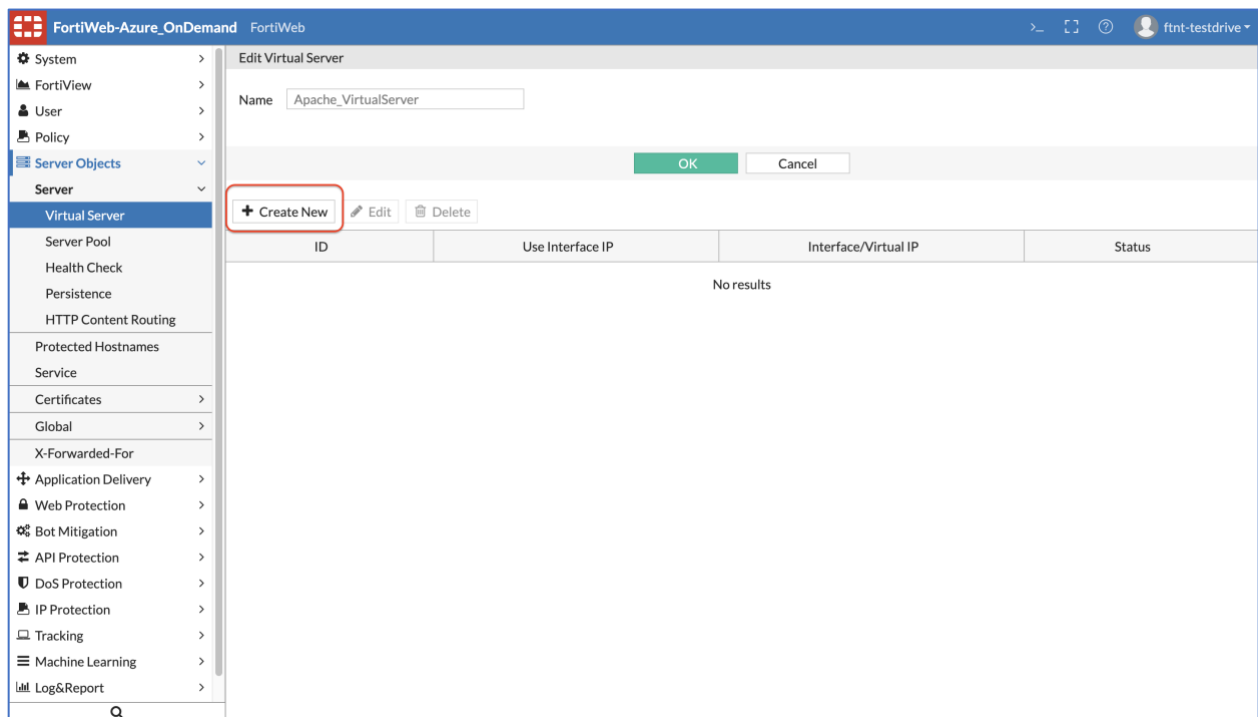
1. Now we will need to create the Virtual Server IP on which the Traffic destined for server pool member arrives. When FortiWeb receives traffic destined for a Virtual server it can then forward to its pool members.



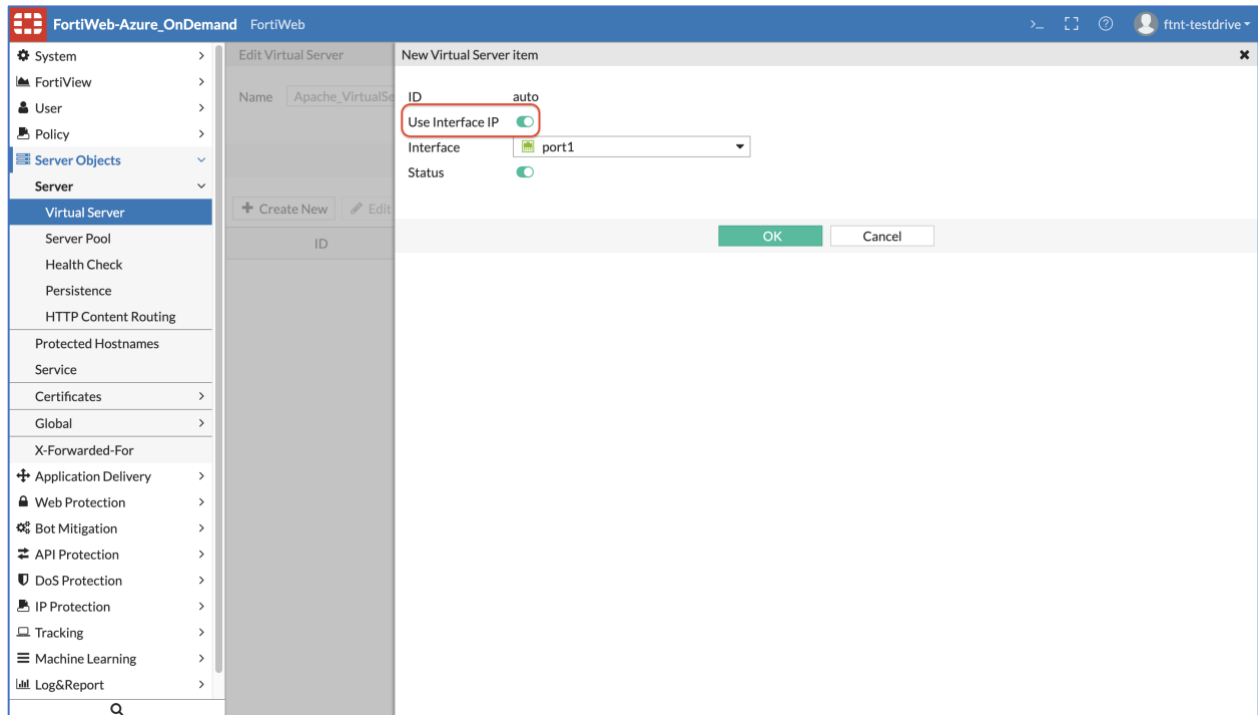
2. Enter the name for the Virtual Server and click OK



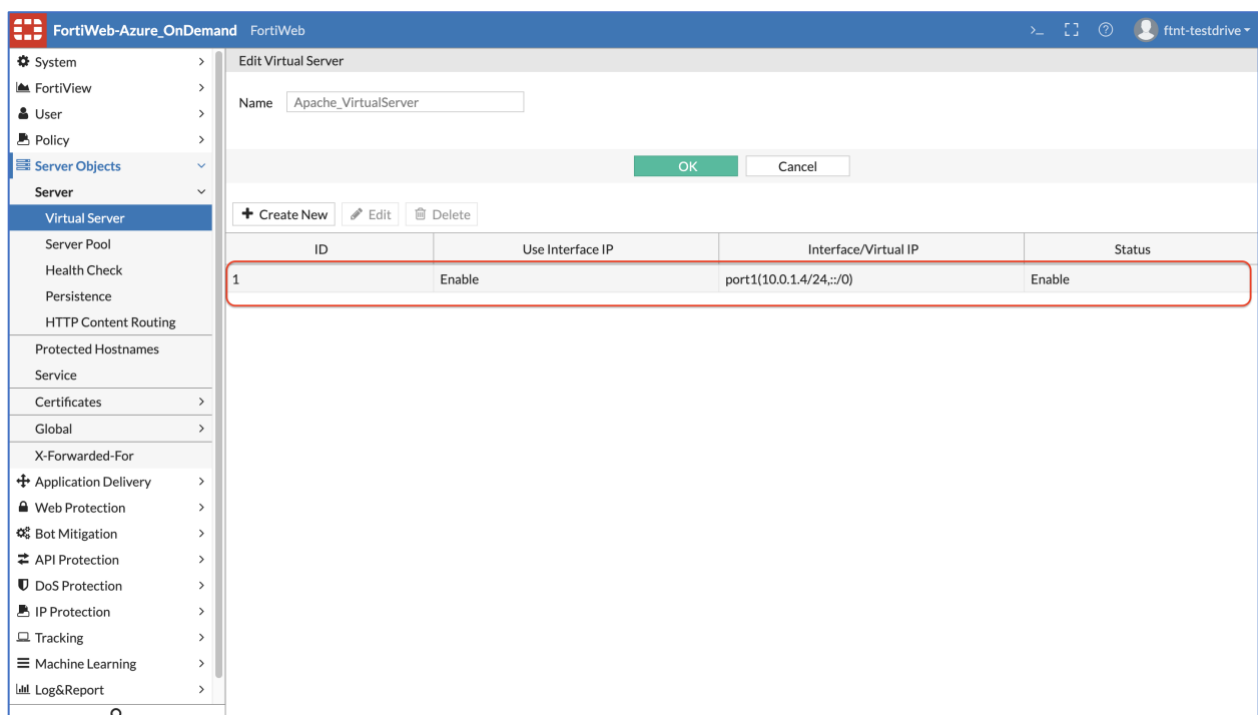
3. Click Create new as shown below to now create Virtual server item.



- 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 interface IP", a drop down with interfaces will appear. Select Port1 as the interface for this Virtual Server item and click OK.



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

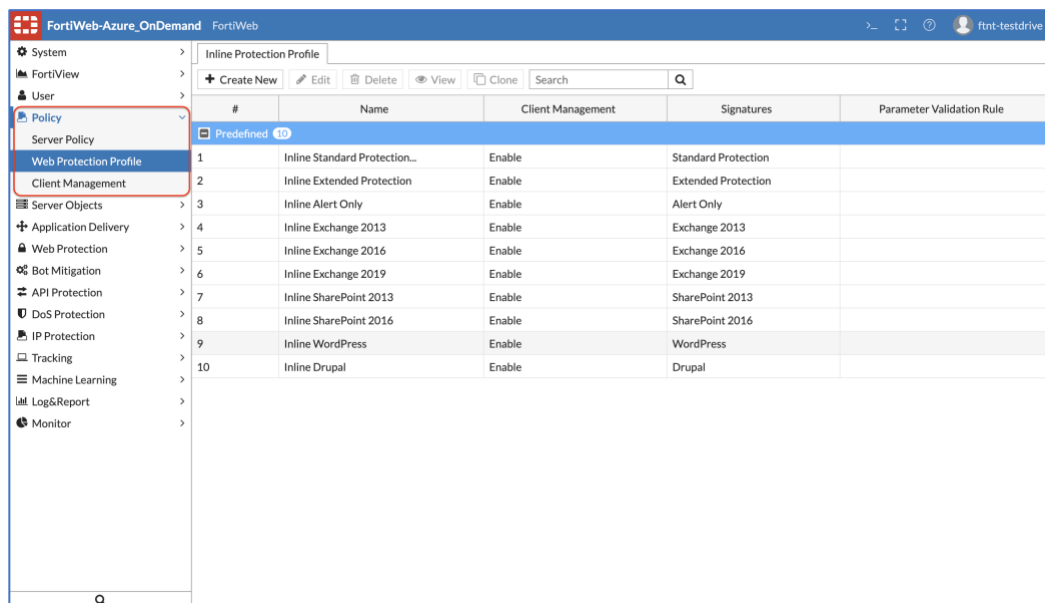


TASK 5 – CREATE WEB PROTECTION PROFILE

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

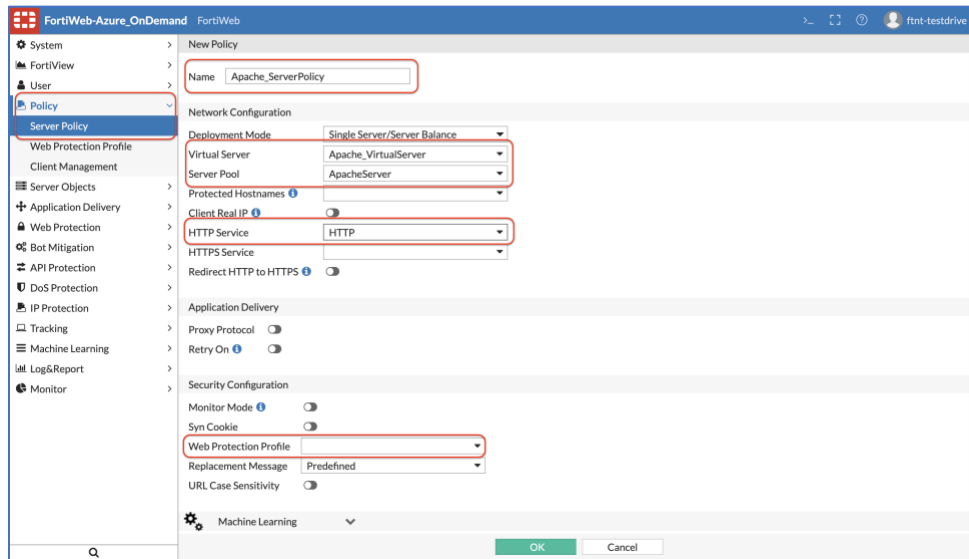


The screenshot shows the FortiWeb-Azure_OnDemand interface. On the left, a navigation menu is visible with categories like System, FortiView, User, Policy, Server Objects, Application Delivery, Web Protection, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Machine Learning, Log&Report, and Monitor. The 'Policy' category is expanded, and 'Web Protection Profile' is selected. The main area displays a table of predefined protection profiles.

#	Name	Client Management	Signatures	Parameter Validation Rule
Predefined 10				
1	Inline Standard Protection...	Enable	Standard Protection	
2	Inline Extended Protection	Enable	Extended Protection	
3	Inline Alert Only	Enable	Alert Only	
4	Inline Exchange 2013	Enable	Exchange 2013	
5	Inline Exchange 2016	Enable	Exchange 2016	
6	Inline Exchange 2019	Enable	Exchange 2019	
7	Inline SharePoint 2013	Enable	SharePoint 2013	
8	Inline SharePoint 2016	Enable	SharePoint 2016	
9	Inline WordPress	Enable	WordPress	
10	Inline Drupal	Enable	Drupal	

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

2. 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



TASK 7 – PERFORM AN ATTACK

Perform an Attack

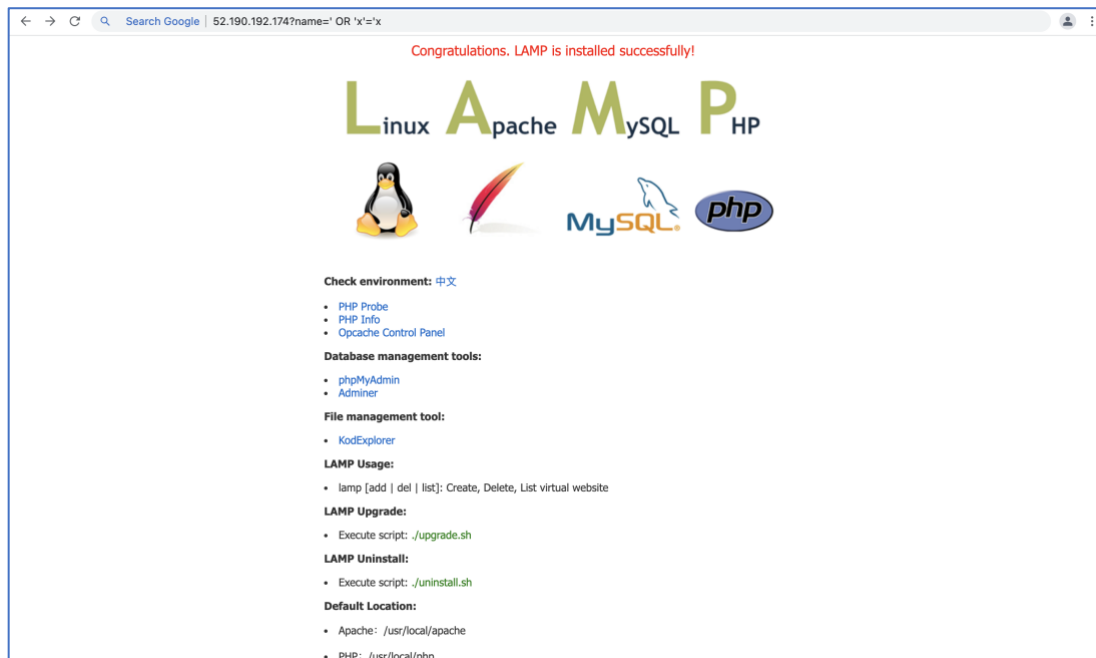
1. Now let's Navigate to the browser and type the Public IP assigned to your FortiWeb instance to get to the web browser. <http://FortiWebIP>



2. 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.

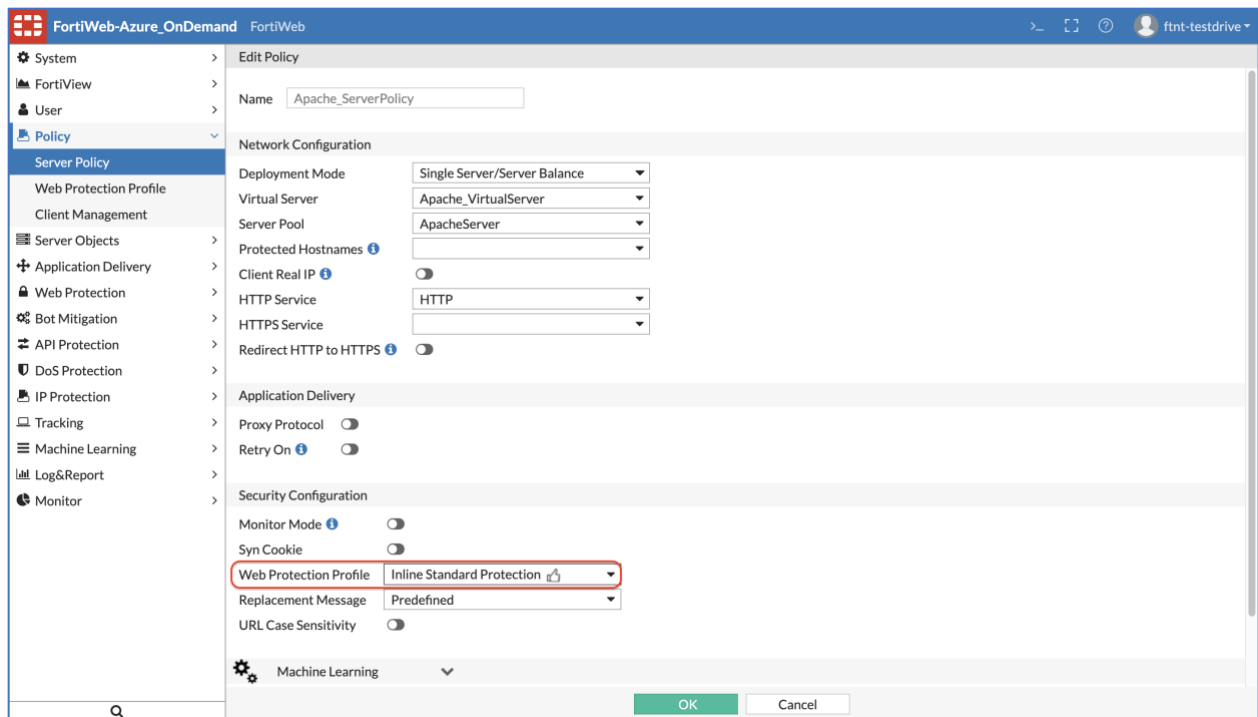


TASK 8 – PROTECT WEB SERVER FROM ATTACK

Protect the Web Server

1. We will now attach the FortiWeb protection profile.

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



2. 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.

