
TEST DRIVE
Fortinet Test Drive for Microsoft Azure

Contents

PREFACE

Fortinet's test drive for Microsoft Azure enables customers to rapidly try FortiGate Enterprise Firewall features, using Microsoft Azure cloud infrastructure-as-a-service (IaaS) services to deploy advanced firewall and threat prevention technology from Fortinet. The key use cases include: building secure isolated virtual networks with one's own IP addresses, hybrid cross premises networking / hybrid networking, and site-to-site or point-to-site VPN. The Azure test drive focuses on demonstrating how High Availability can pass traffic simultaneously or via a dedicated route in Microsoft Azure with FortiGate virtualized firewall appliances.

VERSIONING

FortiGate Appliance version 5.2.3

COMPONENTS

Azure Load Balancer – Abstracted Azure resource, which is scalable and resilient. Dynamically splits traffic between the two FortiGate firewall appliances.

Virtual Network – 10.1.0.0/16, also known as VNET

Public Facing Network – 10.1.0.0/24

Protected Network – 10.1.1.0/24

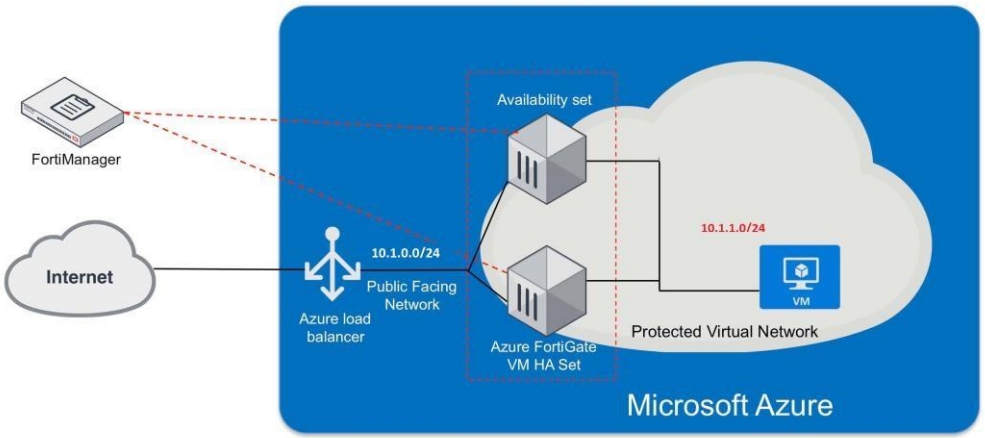
Availability Set – Method of grouping resources within Azure to ensure that they are hosted on separate physical hardware so that at any given time (even during upgrades and maintenance) at least one of the set will remain up.

FortiGate – Azure certified virtual appliance running the same OS that is used on our hardware appliances. These will be referenced as FortiGate-A and FortiGate-B.

FortiManager – Dedicated policy & configuration manager that is used to keep the configuration in sync between the two FortiGate appliances.

DEPLOYMENT

Utilize the FortiGate HA template, which is available in the Microsoft Azure Marketplace to deploy the network resources and FortiGate appliances as depicted in the diagram below.



CONFIGURATION

Azure Load Balancer

All traffic coming from outside of Azure will pass through the Azure load balancer first. The load balancer uses NAT/PAT to connect a single public IP address to the Azure VNET. Within the Azure portal there are two options for configuring these NAT rules. The first is called “Inbound NAT rules.” The second is termed “Load balancing rules.” This is already pre-configured.

Inbound NAT Rules

These rules are applied to a specific host and are not load balanced. As such, these are typically used for management. The template uses ports 443 and 22 for management of FortiGate-A. Ports 8443 and 8022 are similarly directed at FortiGate-B. Once the FortiGate firewall appliances are configured, you can change these ports. For example, if you want to use port 443 for internal web services, you could configure an alternate port on FortiGate-A for management, and modify this rule to use that new port. Once you change the port here, you can then create a new

Load balancing rule to direct 443 to the pair for FortiGate appliances.

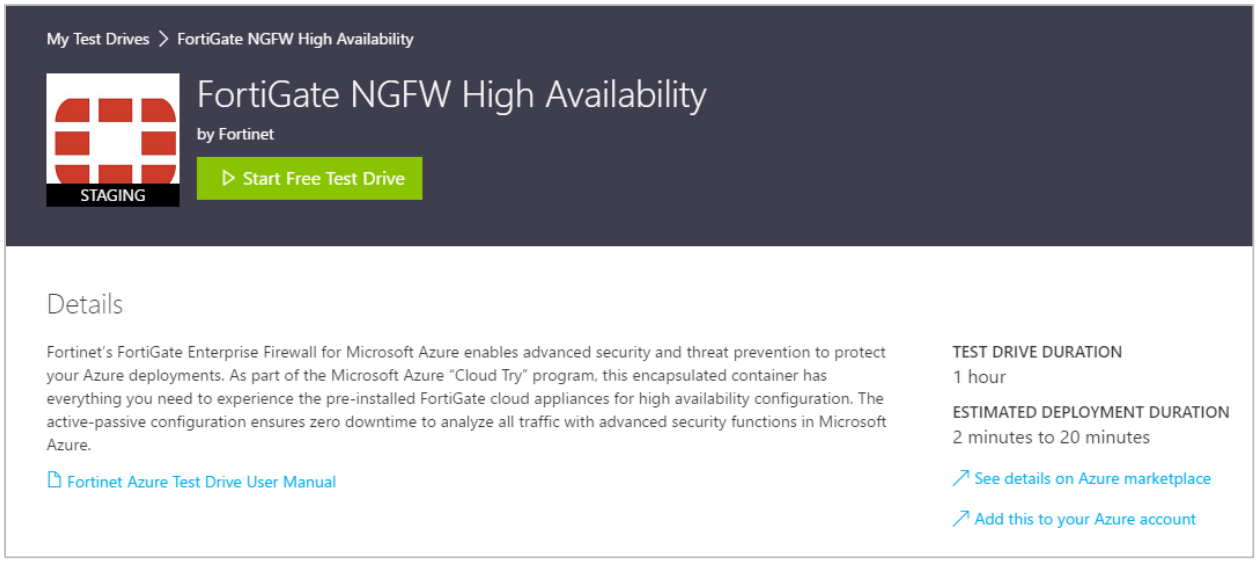
Load Balancing Rules

These rules also use PAT, but rather than being directed at a specific host, they are directed at a backend pool. In this case, the pool consists of FortiGate-A and FortiGate-B. Referencing the above example – after you have freed up port 443, you would create a new Load balancing rule, configured on port 443 and directed to the FortiGate backend pool.

I. Log in for the Fortinet Azure test drive:

Before you can access the test drive, make sure to log in with the required details on the welcome page (E.g. Microsoft Account, etc).

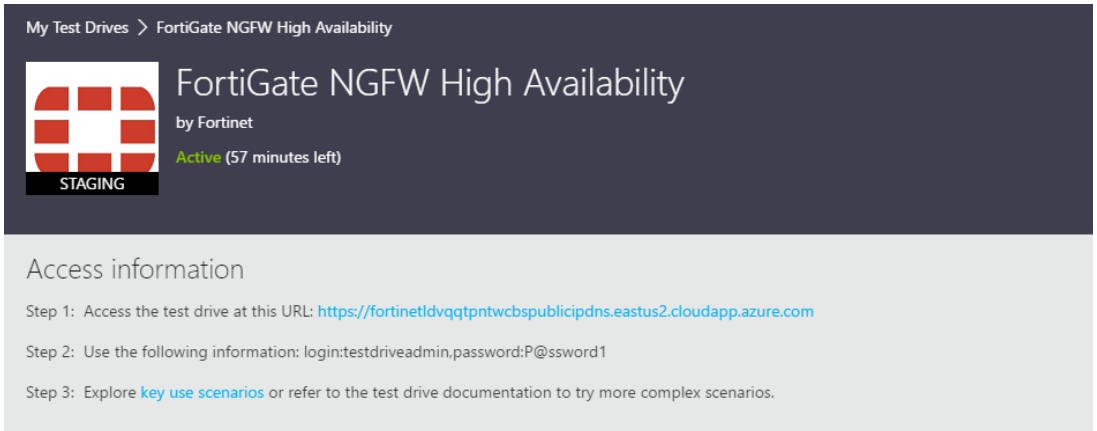
Once you are signed in, you will see the launch screen, shown below. From here, you're ready to launch the test drive!

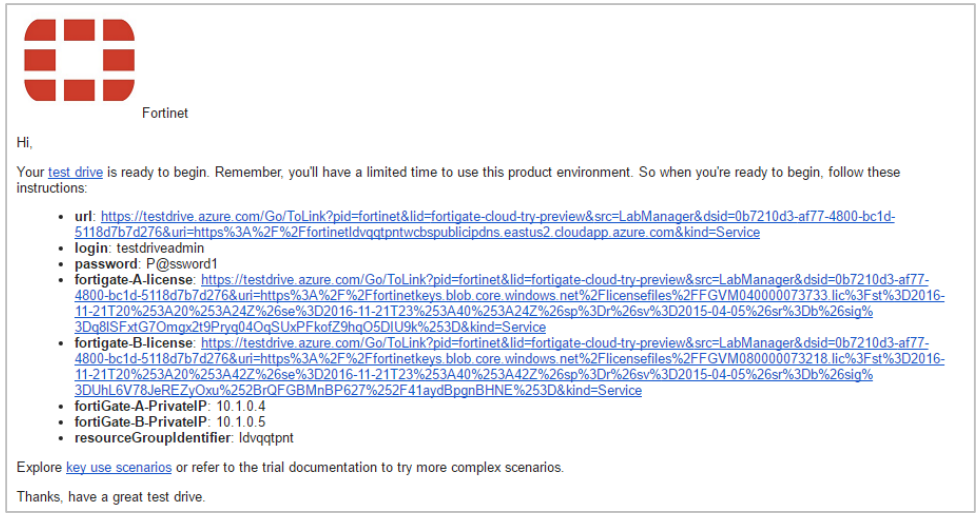


Once you select the 'Start Free Test Drive' button to deploy the test drive, the page will show a progress bar until the test drive is ready. Once ready, the remaining test drive period will be shown at the top of the page, and the credentials needed to access the test drive will be displayed. The credentials are also sent to you via email, so please be sure to check your inbox to make sure you have all the details needed.

Logging in to the test drive:

Once the test drive is launched, use the **URL**, **Login** and **Password** from the test drive launch page, or from the email you received once the test drive was created. (Shown below)





Fortinet

Hi,

Your test drive is ready to begin. Remember, you'll have a limited time to use this product environment. So when you're ready to begin, follow these instructions:

- **url**: https://testdrive.azure.com/Go/ToLink?pid=fortinet&lid=fortigate-cloud-try-preview&src=LabManager&dsid=0b7210d3-af77-4800-bc1d-5118d7b7d276&uri=https%3A%2F%2Ffortinetldvqqtpntwcbspublicipdns.eastus2.cloudapp.azure.com&kind=Service
- **login**: testdriveadmin
- **password**: P@ssword1
- **fortigate-A-license**: https://testdrive.azure.com/Go/ToLink?pid=fortinet&lid=fortigate-cloud-try-preview&src=LabManager&dsid=0b7210d3-af77-4800-bc1d-5118d7b7d276&uri=https%3A%2F%2Ffortinetkeys.blob.core.windows.net%2Flicensefiles%2FFGVM040000073733.lic%3Fst%3D2016-11-21T20%253A20%253A24Z%26se%3D2016-11-21T23%253A40%253A24Z%26sp%3Dr%26sv%3D2015-04-05%26sr%3Db%26sig%3Dq8lSFxtG7Omgx2t9Pryq04OqSUxPFkofZ9hqO5DIU9k%253D&kind=Service
- **fortigate-B-license**: https://testdrive.azure.com/Go/ToLink?pid=fortinet&lid=fortigate-cloud-try-preview&src=LabManager&dsid=0b7210d3-af77-4800-bc1d-5118d7b7d276&uri=https%3A%2F%2Ffortinetkeys.blob.core.windows.net%2Flicensefiles%2FFGVM080000073218.lic%3Fst%3D2016-11-21T20%253A20%253A42Z%26se%3D2016-11-21T23%253A40%253A42Z%26sp%3Dr%26sv%3D2015-04-05%26sr%3Db%26sig%3DUhL6V78JeREZyOxu%252BrQFGBMnBP627%252F41aydBpgnBHNE%253D&kind=Service
- **fortiGate-A-PrivateIP**: 10.1.0.4
- **fortiGate-B-PrivateIP**: 10.1.0.5
- **resourceGroupIdentifier**: ldvqqtpnt

Explore key use scenarios or refer to the trial documentation to try more complex scenarios.

Thanks, have a great test drive.

Both the environment log and the email contain the **URL**, **login id**, **password**, two **license file URLs,** and **private IP** of both A & B FortiGates.

Once you've logged in to the test drive, you will create a policy on FortiGate-A (and FortiGate-B) to allow outbound internet connectivity (be sure to enable NAT using the outgoing interface address. To do this, you can:

- Connect to FortiGate-A via https on default port 443 (https://dnsURL)
- Connect to FortiGate-B via https on port 8443 (https://dnsURL:8443)

For example, use the URL provided in the environment window and in the email to connect to FortGate-A (on port 443 by default), and use the same URL but with **:8443** appended at the end to connect to Fortigate-B.

Note: these ports are configured in the Azure Load Balancer Inbound NAT rules and can be changed (for instance if you want to use port 443 for internal resources). Additionally, you can add multiple frontends to the load balancer each with its own public IP address. **Follow the instructions in Step-1 below to get started!**

FORTIGATE CONFIGURATION

FortiGate –A

Step-1:

Licenses

The first step of configuration is to install a license on each FortiGate. Connect to the web-based management interface by entering the **public URL** (provided in the Env Log and email under “url”) assigned to the Azure Load Balancer into a web browser.

The default URL will connect you to **Fortigate-A**. To connect to Fortigate-B, enter the same URL but add “**:8443**” at the end of it. These will be in two separate browser windows/tabs.

Note: You may receive a warning message stating your connection is not secure. Please disregard this and select the option to Proceed.

Use the username and password to login for both FortiGates. (shown below)

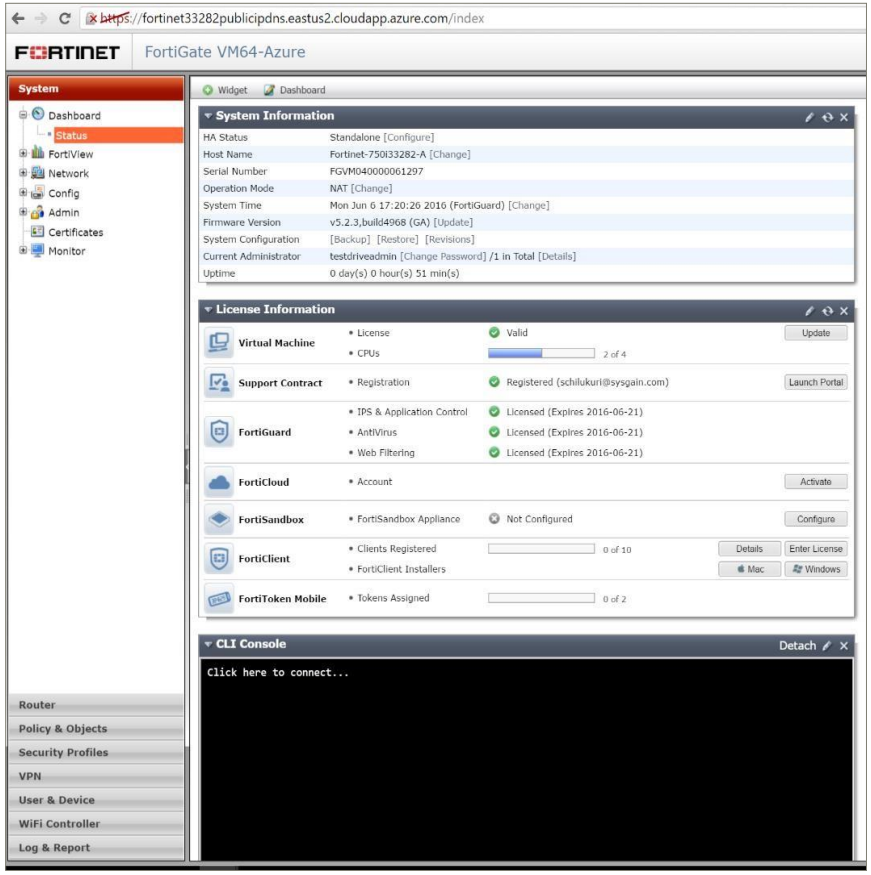


Fig. 1

Once connected, you will be prompted to install a license file:

Download the license files from the "**fortigate-A-license**" and "**fortigate-Blicense**" links provided in the email. As their names suggest, there is one for each FortiGate.

Upload each license file on the corresponding web pages, and wait for the FortiGate to reboot and connect to the FortiGuard services. From here, continue the test drive in **FortiGate A**. Full FortiGuard synchronization can take up to 30 minutes. However, you should be able to connect and continue configuration within about 5 minutes.

Note: if it takes an abnormally long time to reboot, try manually refreshing the page. You may be prompted to upload the file again.

Once the system is restarted, it will ask for the login credentials again. Enter those credentials and select 'login'. Then you will see a screen like the one shown in Fig. 1 (above).

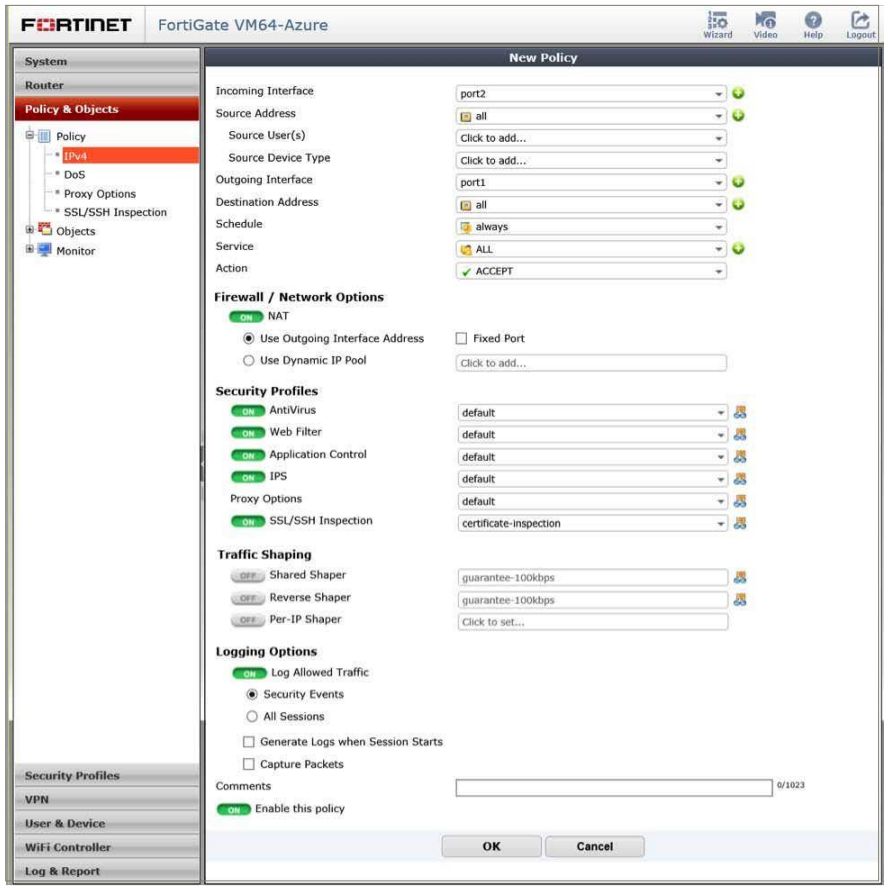
If you see an alert message like the one shown below appear, please select 'Later' and proceed with the test drive.

Step-2

Outbound Communication

In order to allow outbound communication from hosts on the Protected Network to the Internet or other external hosts, you will need to configure a policy:

1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Policy**" and "**IPv4**".
3. Click the "**Create New**" button in the top tool bar.
4. Select **Port2** for "**Incoming Interface**".
5. For **Source** address you can be as granular as you like. In this example, we'll use "**all**".
6. Select **Port1** for "**Outgoing Interface**".
7. For **Destination address** select "**all**" – again you can be as granular as you like here.
8. For **Service** select "**ALL**".
9. Ensure that **NAT** is **enabled.**
10. Select all **Security Profiles.**
11. Click "**Okay**" at the bottom of the screen.

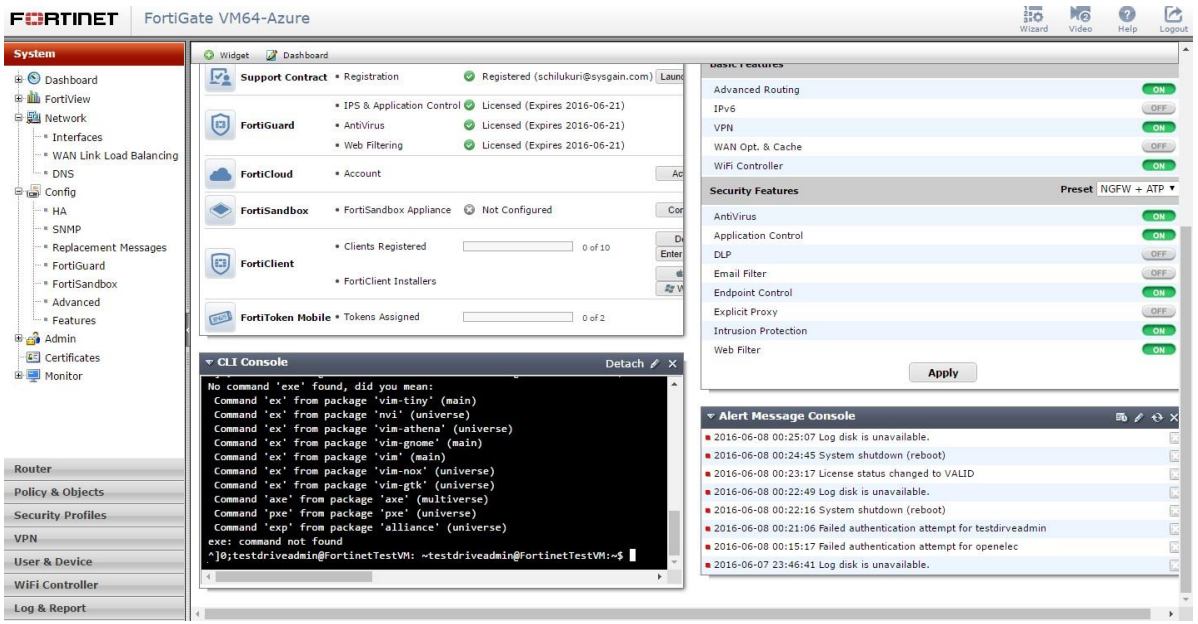


For additional information on granular configuration, security profiles, etc., please see the FortiOS Handbook: http://docs.fortinet.com/d/fortigate-for-tios-handbook-the-complete-guide-to-fortios-5.2

Step 3:

Install Apache2 in FortiGate-A

Select the **System** tab from the left-side navigation column. This will take you back to the dashboard:



Using the **CLI Console** window in the lower left corner of the main dashboard screen, enter the commands below to SSH into the Ubuntu VM from FortiGate-A or FortiGate-B console: (***Note***: If the CLI fails to connect from the Fortigate (A/B) you are using, please try using the console on the other Fortigate page (A/B) , this should work.)

1. *Type **"exe ssh testdriveadmin@10.1.1.6", hit Enter***
2. *Enter the same **password** used at the start of this test drive.*
3. *Type **"sudo apt-get install apache2", hit Enter***
4. *Type **"Y"** and hit **Enter** to continue*
5. ***Verify that Apache is functioning** by exiting the SSH session (type '**exit**' in the console window and hit **Enter**) and then **establishing a telnet session to port***
   i. ***80: "exe telnet 10.1.1.6 80".** If Apache is working, you should see the message below **("Connected to 10.1.1.6.")***

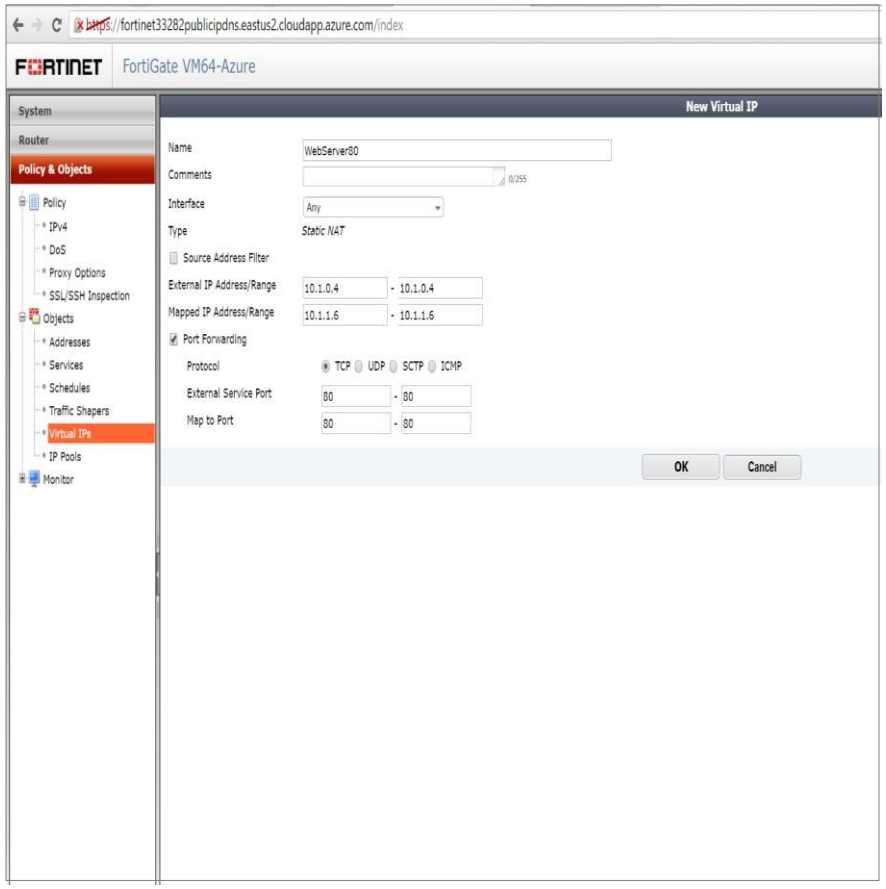
```
Fortinet-750i33282-B # exe telnet 10.1.1.6 80
Trying 10.1.1.6...
Connected to 10.1.1.6.
```

Note: If Apache fails to install, try logging out and then logging back in to the FortiGate, then try again. If it is still failing, enter "***sudo apt-get update"*** before step 3, above.

Step-4

Inbound Communication

To enable traffic coming from the internet, you will need to configure **PAT** on the FortiGates. The first step will be to create a Virtual IP:



1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Objects**" and "**Virtual IPs**".
3. Click the "**Create New**" button in the top tool bar.
4. Type a name. In this example, we'll use "**WebServer80**".
5. Select **Any** under "**Interface**".
6. Use the IP address of the FortiGate you are using (A or B) for the **External IP Address/Range** (type it twice as shown).

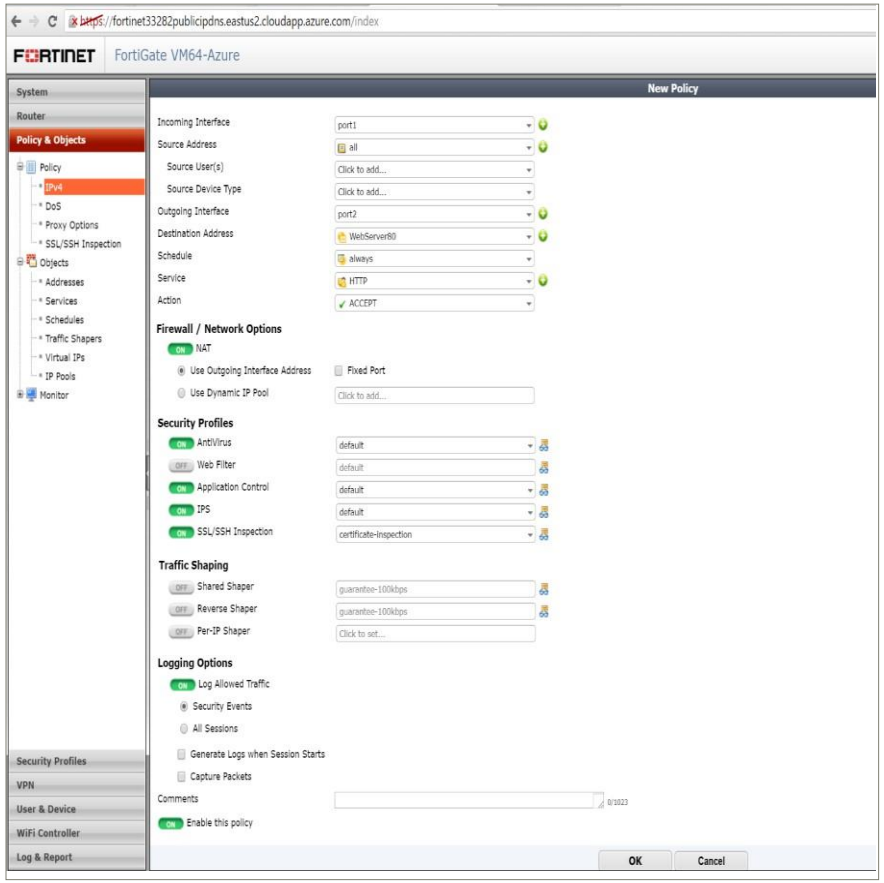
   (This will be the IP address shown as either "**fortiGate-A-PrivateIP**" or "**fortiGate-B-PrivateIP**" in the environment log and email).
7. For the "**Mapped IP Address/Range**," use the IP address of your **internal hos**t (10.1.1.6).
8. Select the checkbox next to "**Port Forwarding**".
9. Select the **Protocol** you wish to use.
10. Type in the **port** you wish to use. This can be a range or a single port. In this example, we'll use **80**. If you wish to forward the external port 80, you will need to change the management port of FortiGate-A and the Inbound NAT Rule (both processes are described above). The external port can be mapped to a different internal port here if desired.
11. Click "**Okay**" at the bottom of the page.

Step-5

Creating new IPV4 Policy in FortiGate-A:

Once you have the Virtual IP configured, you need to create a new policy:

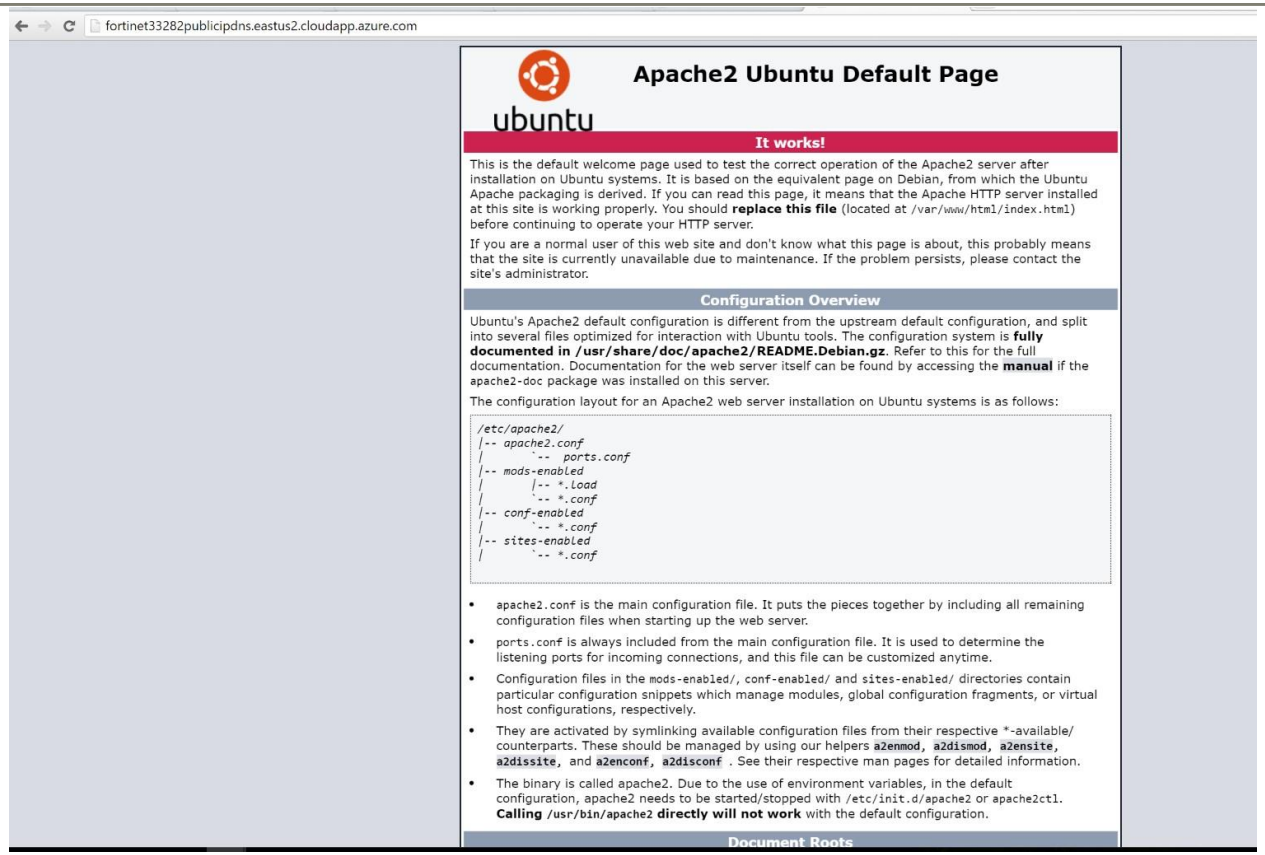
1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Policy**" and "**IPv4**".
3. Click the "**Create New**" button in the top tool bar.
4. Select **Port1** for "**Incoming Interface**".
5. For **Source address** you can be as granular as you like. In this example, we'll use "**all**".
6. Select **Port2** for "**Outgoing Interface**".
7. For **Destination address** select the name of the **Virtual IP** that you created ("WebServer80")
8. For Service select "**HTTP**".
9. Ensure that **NAT** is **enabled.**
10. Select all **Security Profiles** *except* **Web Filter.**
11. Click "**Okay**" at the bottom of the page.



Step-6

Connect to **port 80** on the DNS URL (same URL as used above), be sure to use **http://** as most browsers will attempt to pretend https:// , since it's cached.

[Example: http://fortinet33282publicipdns.eastus2.cloudapp.azure.com:80]



If the output is the same as what is shown above, then FortiGate-A is working! Next, you will want to configure FortiGate-B.

FortiGate-B :

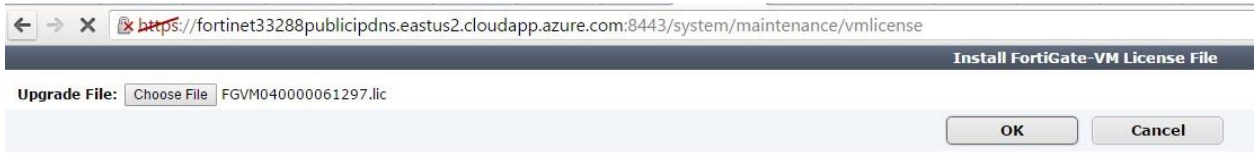
Step-1:

Logging In

Follow the same steps as FortiGate-A:

Copy the URL provided in the environment log and email and paste it in any browser, then add ":8443" to the end of it. Enter the login credentials which are provided in environment log or email. Ex: (https://dnsURL:8443).

Once you login into the site it will ask to upload license key. If you have not already done this, download the licenses from the provided license URL's, and upload the file.

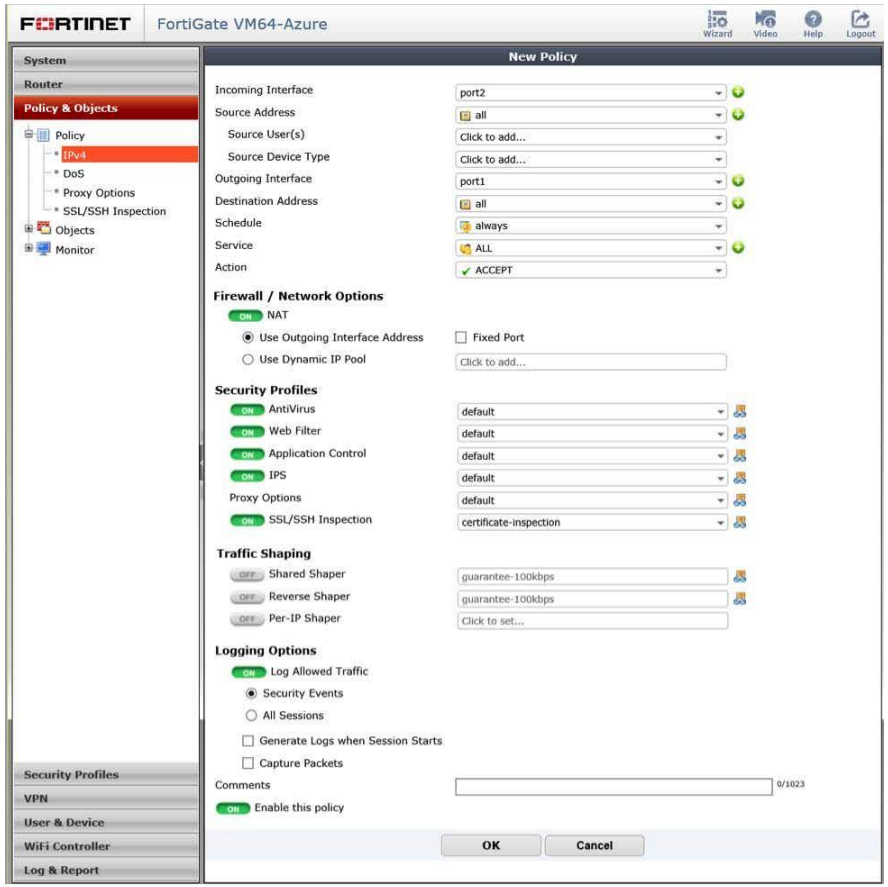


Step-2:

Outbound Communication

Follow the same steps as mentioned in FortiGate-A:

1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Policy**" and "**IPv4**".
3. Click the "**Create New**" button in the top tool bar.
4. Select **Port2** for "**Incoming Interface**".
5. For **Source** address you can be as granular as you like. In this example, we'll use "**all**".
6. Select **Port1** for "**Outgoing Interface**".
7. For **Destination address** select "**all**" – again you can be as granular as you like here.
8. For **Service** select "**ALL**".
9. Ensure that **NAT** is **enabled.**
10. Select all **Security Profiles.**
11. Click "**Okay**" at the bottom of the screen.



Step-3:

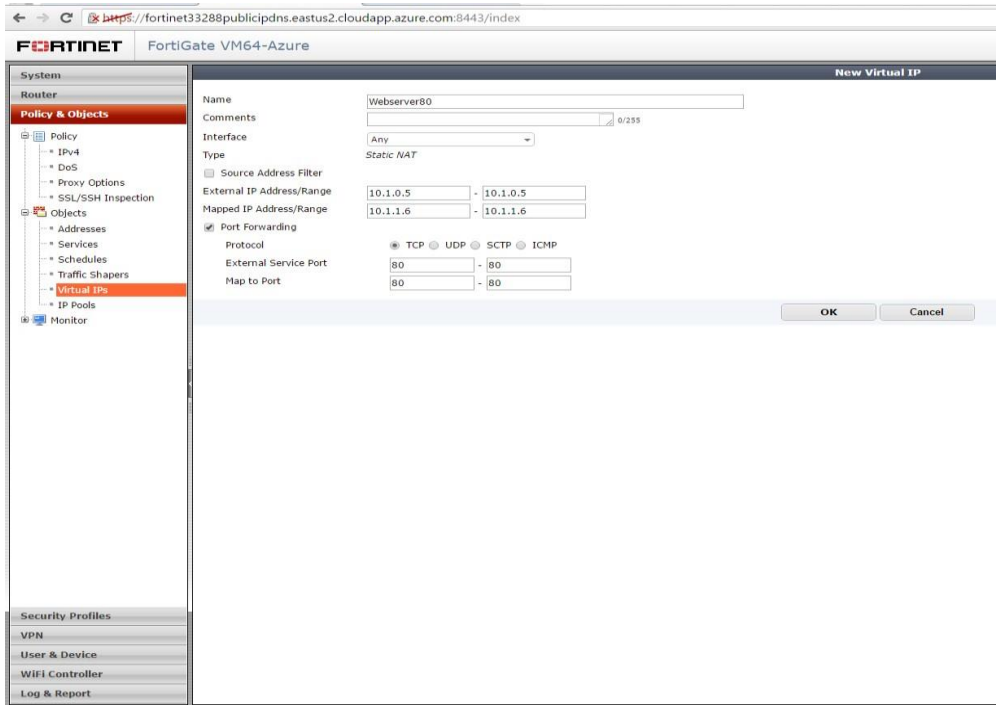
Inbound Communication

Follow the same steps as FortiGate-A…

… **Except for one detail**: modify the **External IP Address/Range** from **10.1.0.4** (FortiGate-A IP) to **10.1.0.5** (FortiGate-B IP).

1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Objects**" and "**Virtual IPs**".
3. Click the "**Create New**" button in the top tool bar.
4. Type a name. In this example, we'll use "**WebServer80**".
5. Select **Any** under "**Interface**".
6. Use the IP address of the FortiGate you are using (A or B) for the **External IP Address/Range** (type it twice as shown).

   (This will be the IP address shown as "**fortiGate-B-PrivateIP**" in the environment log and email).
7. For the "**Mapped IP Address/Range**," use the IP address of your **internal hos**t (10.1.1.6).
8. Select the checkbox next to "**Port Forwarding**".
9. Select the **Protocol** you wish to use.
10. Type in the **port** you wish to use. This can be a range or a single port. In this example, we'll use **80**. If you wish to forward the external port 80, you will need to change the management port of FortiGate-A and the Inbound NAT Rule (both processes are described above). The external port can be mapped to a different internal port here if desired.
11. Click "**Okay**" at the bottom of the page.



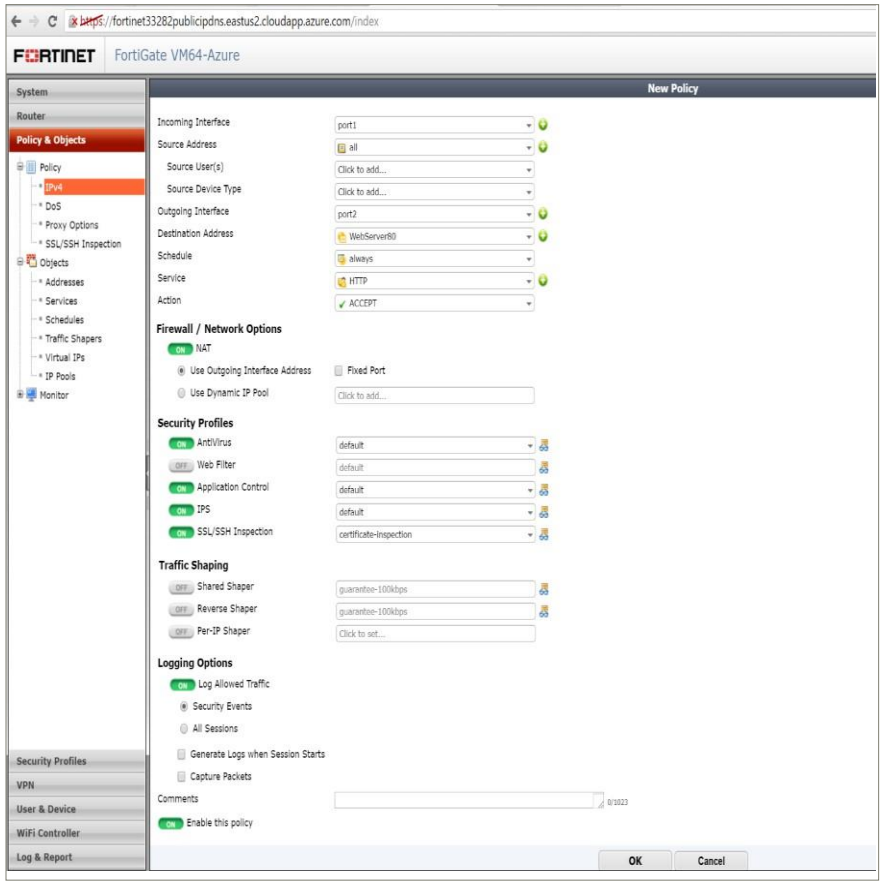
Step-4:

Creating a new IPV4 Policy in FortiGate-B

Follow the same steps as FortiGate-A;

Once you have the Virtual IP configured, you need to create a new policy:

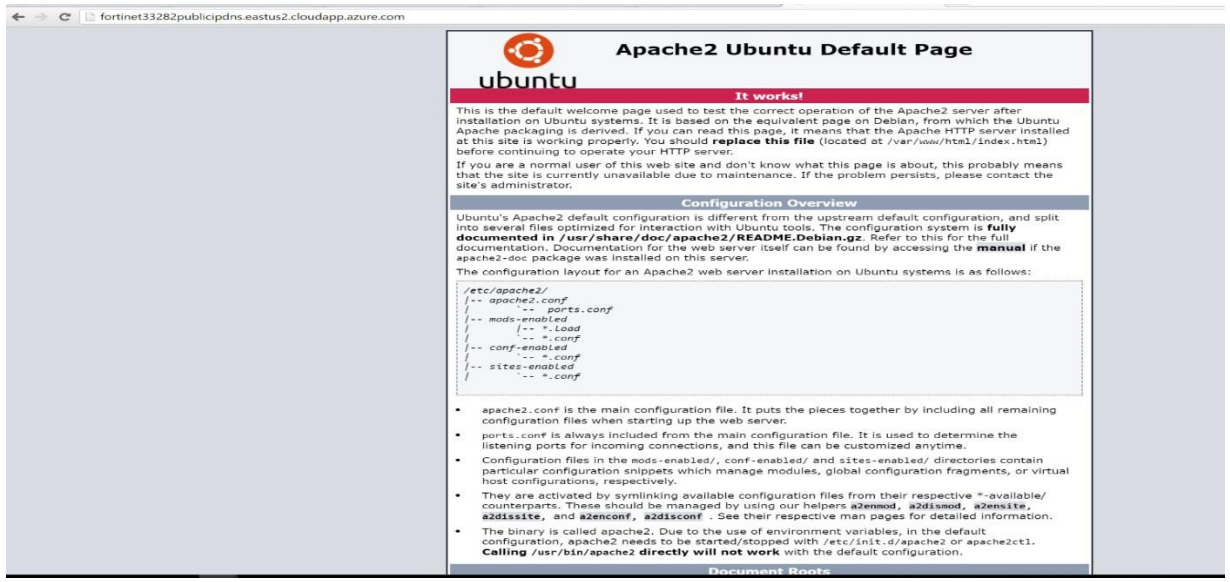
1. Select "**Policy & Objects**" along the left hand side of the management interface.
2. Select "**Policy**" and "**IPv4**".
3. Click the "**Create New**" button in the top tool bar.
4. Select **Port1** for "**Incoming Interface**".
5. For **Source address** you can be as granular as you like. In this example, we'll use "**all**".
6. Select **Port2** for "**Outgoing Interface**".
7. For **Destination address** select the name of the **Virtual IP** that you created ("WebServer80")
8. For Service select "**HTTP**".
9. Ensure that **NAT** is **enabled.**
10. Select all **Security Profiles** *except* **Web Filter.**
11. Click "**Okay**" at the bottom of the page.



Step-5:

Connect to port 80 on DNS URL (same as used above), be sure to use **http://** since most browsers will attempt to pretend https:// since it's cached.

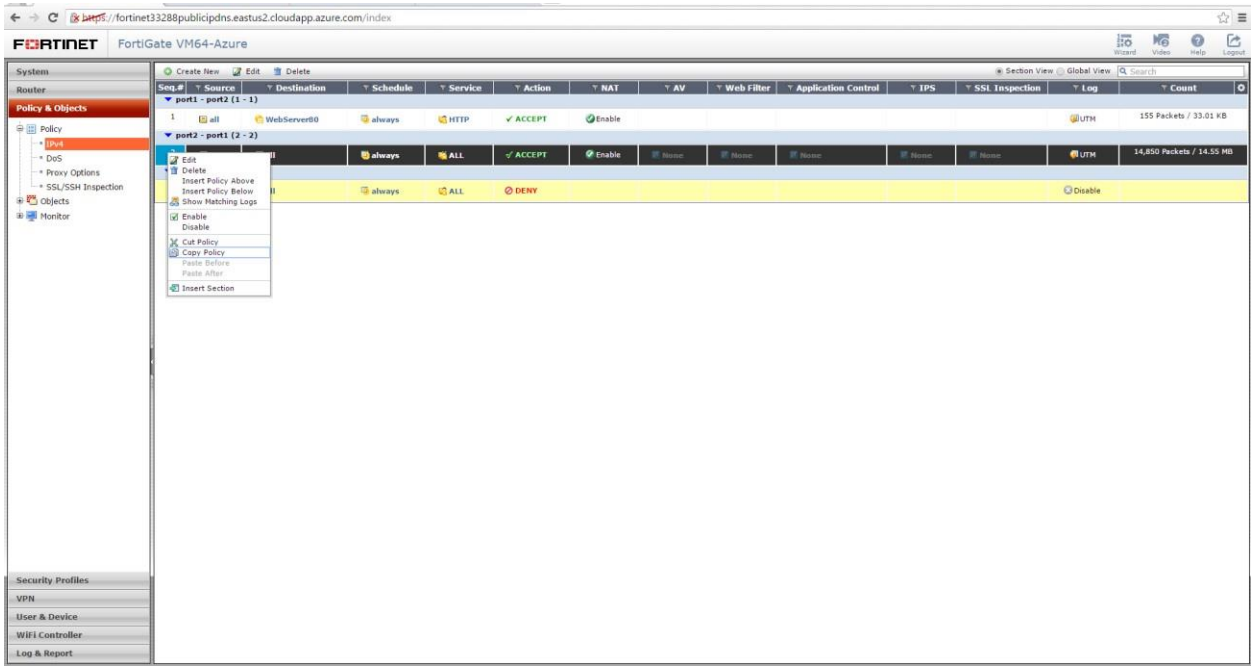
[i.e. http://fortinet33282publicipdns.eastus2.cloudapp.azure.com:80]



If you see the Apache2 Ubuntu Default Page, then this means that both gates are working correctly!

Verification:

- Either in FortiGate-A or Fortigate-B, delete one of the policies under the **Policy and Objects** section, as shown below. Right click on a policy and delete it.
- Also, delete the Virtual IP "**Webserver80**" under the **Objects** section.



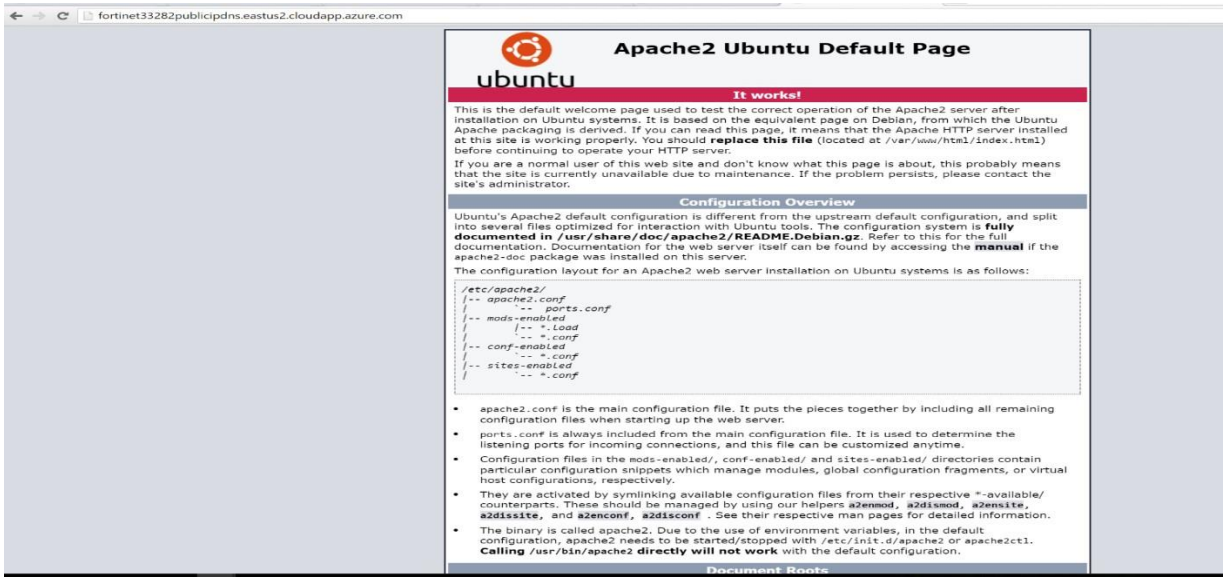
If you delete these in FortiGate-A, it will make it so that FortiGate-A is no longer in connection with the Apache2 web server.

In that case, now FortiGate-B will work and should still be connected with the web server.

You can verify this by performing the same step used before:

Connect to port 80 with the primary DNS URL (same as used above). Be sure to use http:// since most browsers will attempt to use https:// .

[i.e. http://fortinet33282publicipdns.eastus2.cloudapp.azure.com:80]



If you still see the Apache2 Default Page, then FortiGate-B has successfully provided a backup connection to the web server.

Routing

Through the use of the Azure Load Balancer and the bidirectional NAT on the FortiGate appliances (described above), we are able to achieve high availability for incoming connections. For many common services this is adequate. However, for services requiring the ability to create outbound connections like SMTP servers or Web servers that communicate with other databases, etc., there's an additional monitor that needs to be deployed.

In order to force internal-external traffic to route through the FortiGate, we use a feature called User Defined Routes (UDRs). This allows us to specify an alternative router to the default Azure router, but it only allows a single router per route and if that router is not available, the traffic gets dropped. Thus, to support highly available internal > external connections we need to change that UDR. Fortinet and Microsoft are working together to automate this and get deployed via the marketplace template soon. In the interim, the solution that we have tested requires an external A0 sized pair of Ubuntu servers that run a monitor script and change the Azure UDR in the case that FortiGate-A becomes inaccessible.

Support

For more information on troubleshooting your Azure test drive please contact azure@fortinet.com to obtain this script and get further assistance.