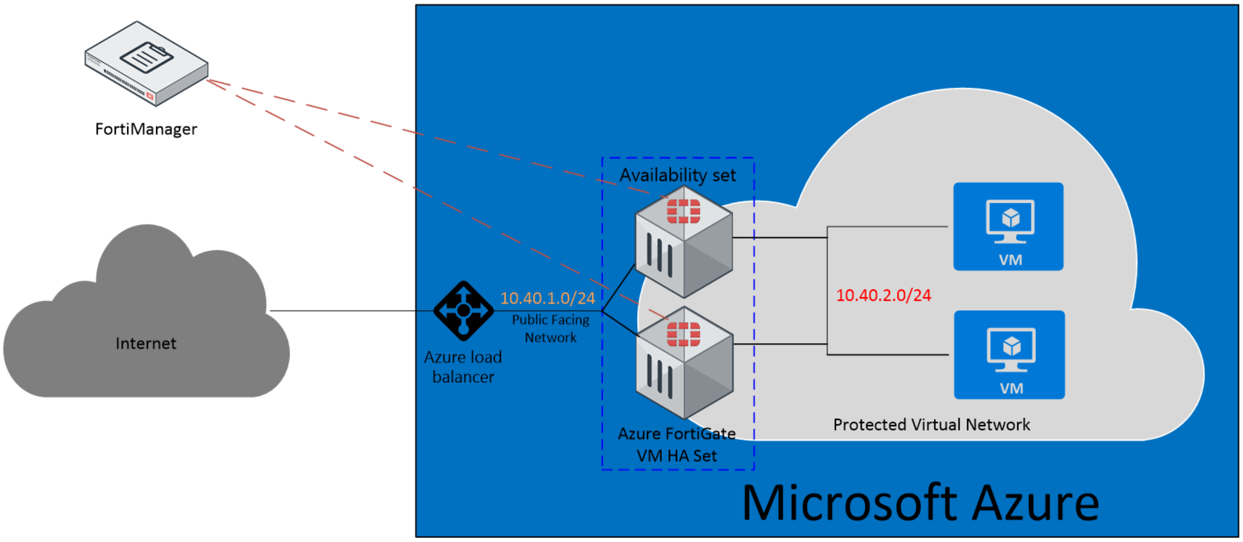
FortiGate scalable HA reference design for MS Azure virtual networks



Components:

Azure Load Balancer – Abstracted Azure resource which is scalable and resilient. Dynamically splits traffic between the two FortiGates.

Virtual Network – 10.40.0.0/16, also known as VNET

Public Facing Network – 10.40.1.0/24

Protected Network – 10.40.2.0/24

Availability Set – Method of grouping resources within Azure to ensure that they are hosted on separate physical hardware in order to ensure 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 which is used on our hardware appliances. These will be referenced as FortiGate-A and FortiGate-B.

FortiManager – Dedicated policy and configuration manager, used to keep the configuration in sync between the two FortiGates.

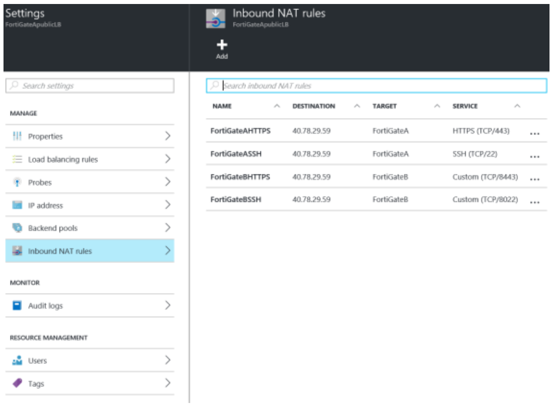
How to deploy:

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

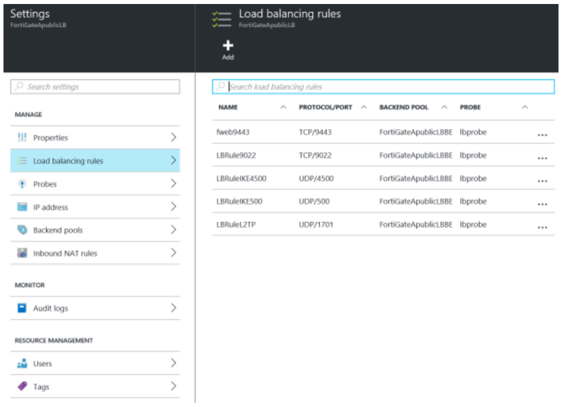
Configuration:

Azure Load Balancer

All traffic coming from outside of Azure will pass through the load balancer first. The load balancer uses Network Address Translation and Port Address Translation (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”



NAME	DESTINATION	TARGET	SERVICE
FortiGateAHTTPS	40.78.29.59	FortiGateA	HTTPS (TCP/443)
FortiGateASSH	40.78.29.59	FortiGateA	SSH (TCP/22)
FortiGateBHTTPS	40.78.29.59	FortiGateB	Custom (TCP/8443)
FortiGateBSSH	40.78.29.59	FortiGateB	Custom (TCP/8022)



NAME	PROTOCOL/PORT	BACKEND POOL	PROBE
fweb9443	TCP/9443	FortiGateApublicLBBE	lbprobe
LBRule9022	TCP/9022	FortiGateApublicLBBE	lbprobe
LBRuleIKE4500	UDP/4500	FortiGateApublicLBBE	lbprobe
LBRuleIKE500	UDP/500	FortiGateApublicLBBE	lbprobe
LBRuleL2TP	UDP/1701	FortiGateApublicLBBE	lbprobe

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 FortiGates 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 of FortiGates.

Load balancing rules

These rules also use PAT, but rather than being directed at a specific host, they are directed at a collection of virtual machines called a backend pool. In this case, the pool consists of FortiGate-A and FortiGate-B. These rules are necessary to provide high availability and load balancing for any given service. 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.

FortiGate Configuration

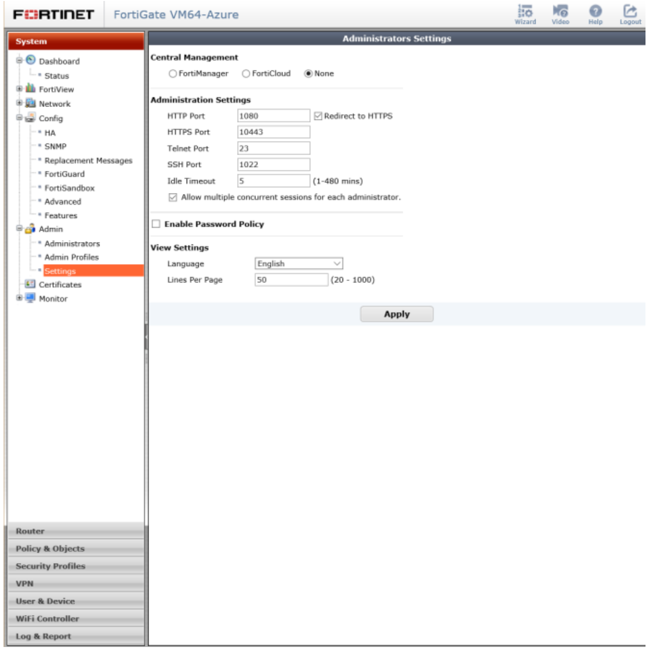
Licenses

The first step of configuration is to install a license. Connect to the web-based management interface at the public IP address assigned to the Azure Load Balancer. This interface will be available via port 443 for FortiGate-A and 8443 for FortiGate-B. Once connected, you will be prompted to install a license file. After you have uploaded the license file, wait for the FortiGate to reboot and connect to the FortiGuard services. Full FortiGuard synchronization can take up to 30 minutes. However, you should be able to connect and continue configuration within about 5 minutes.

Note: The Marketplace template does not come with a license. In order to obtain a license, you will need to work with your Fortinet representative or network security partner. Alternately, you can email azure@fortinet.com

Management Ports

If you would like to change the management ports in order to allow those ports to be forwarded to internal resources, select System -> Admin -> Settings and adjust accordingly.



Administrators Settings

Central Management

○ FortiManager ○ FortiCloud ● None

Administration Settings

HTTP Port 1080 ☑ Redirect to HTTPS

HTTPS Port 10443

Telnet Port 23

SSH Port 1022

Idle Timeout 5 (1-480 mins)

☑ Allow multiple concurrent sessions for each administrator.

□ Enable Password Policy

View Settings

Language English

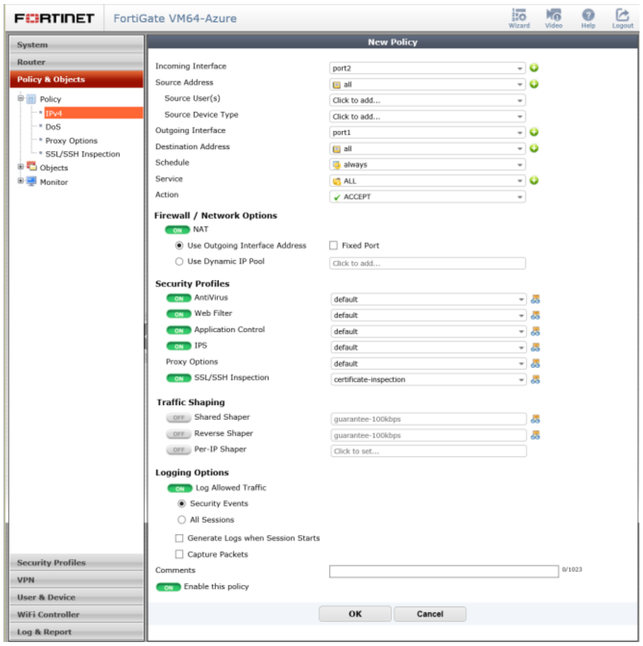
Lines Per Page 50 (20 - 1000)

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 your desired Security Profiles

11. Click “Ok” at the bottom



New Policy

Incoming Interface	port2
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

ON NAT

● Use Outgoing Interface Address □ Fixed Port

○ Use Dynamic IP Pool Click to add...

Security Profiles

ON AntiVirus	default
ON Web Filter	default
ON Application Control	default
ON IPS	default
Proxy Options	default
ON SSL/SSH Inspection	certificate-inspection

Traffic Shaping

OFF Shared Shaper	guarantee-100kbps
OFF Reverse Shaper	guarantee-100kbps
OFF Per-IP Shaper	Click to set...

Logging Options

ON Log Allowed Traffic

● Security Events

○ All Sessions

□ Generate Logs when Session Starts

□ Capture Packets

Comments 0/1023

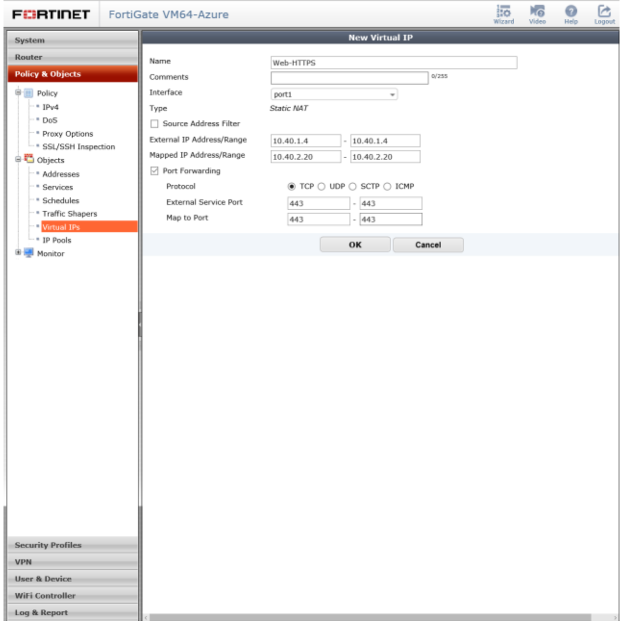
ON Enable this policy

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

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 my example, I’m using Web-HTTPS
5. Select port1 under “Interface”
6. Use the IP address of port1 for the External IP Address/Range (type it twice).
7. For the “Mapped IP Address/Range,” use the IP address of your internal host (again type it twice).
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 the example I’m using 443. If you wish to forward the external port 443, 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 “Ok” at the bottom

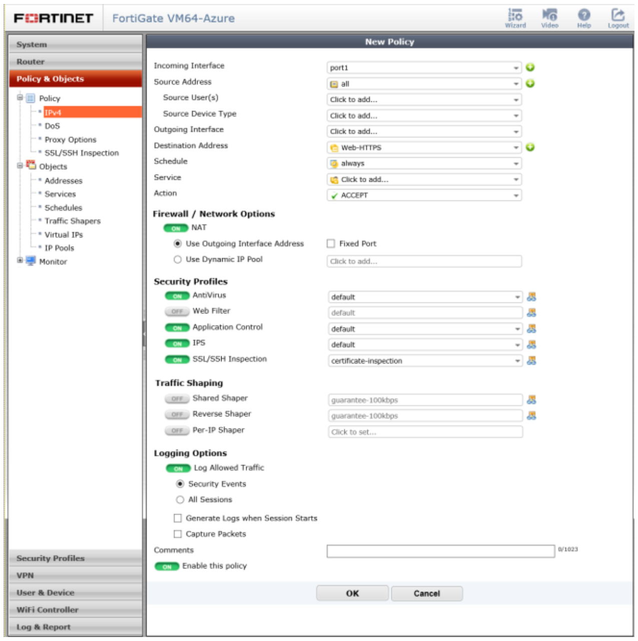


New Virtual IP

Name: Web-HTTPS
Comments: 0/255
Interface: port1
Type: Static NAT
□ Source Address Filter
External IP Address/Range: 10.40.1.4 - 10.40.1.4
Mapped IP Address/Range: 10.40.2.20 - 10.40.2.20
☑ Port Forwarding
Protocol: ● TCP ○ UDP ○ SCTP ○ ICMP
External Service Port: 443 - 443
Map to Port: 443 - 443

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 Port1 for “Outgoing Interface”
7. For Destination address select the name of the Virtual IP that you created
8. For Service select “ALL”
9. Ensure that NAT is enabled
10. Select your desired Security Profiles
11. Click “Ok” at the bottom



New Policy

Incoming Interface	port1
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	Click to add...
Destination Address	Web-HTTPS
Schedule	always
Service	Click to add...
Action	✓ ACCEPT

Firewall / Network Options

ON NAT

● Use Outgoing Interface Address □ Fixed Port

○ Use Dynamic IP Pool Click to add...

Security Profiles

ON AntiVirus	default
OFF Web Filter	default
ON Application Control	default
ON IPS	default
ON SSL/SSH Inspection	certificate-inspection

Traffic Shaping

OFF Shared Shaper	guarantee-100kbps
OFF Reverse Shaper	guarantee-100kbps
OFF Per-IP Shaper	Click to set...

Logging Options

ON Log Allowed Traffic

● Security Events

○ All Sessions

□ Generate Logs when Session Starts

□ Capture Packets

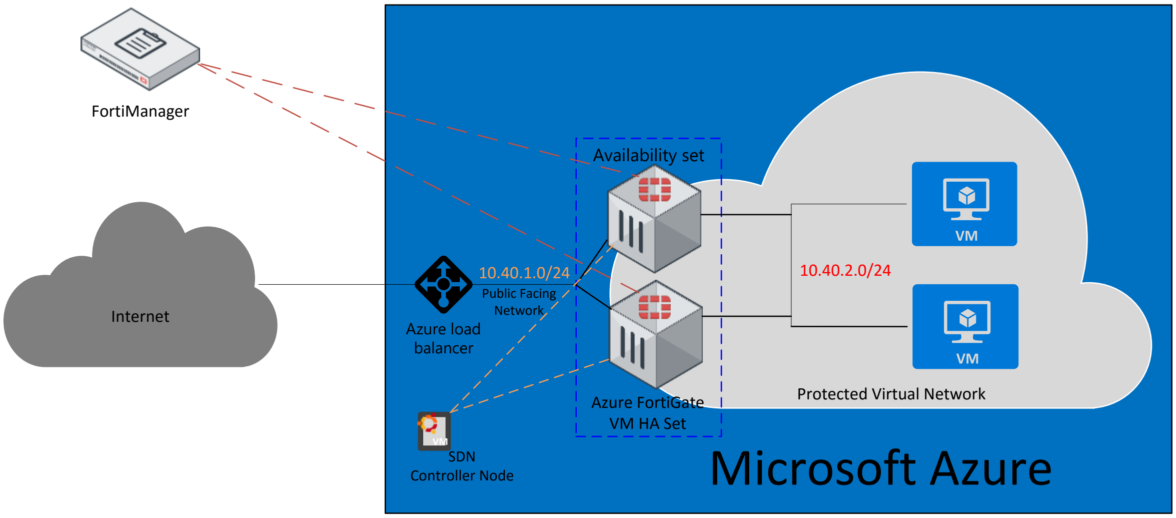
Comments 0/1023

ON Enable this policy

Routing

Through the use of the Azure Load Balancer and the source NAT on incoming traffic to the FortiGates (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 which 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 an Azure feature called User Defined Routes (UDRs). This allows us to specify an alternative 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. We are working with Microsoft on various ways to do this and hope to have an automated solution that gets deployed via the marketplace template soon. In the interim, the solution that we have tested requires an external A0 sized Ubuntu server to act as a Software Defined Network (SDN) controller. It does so by running a monitor script and changing the Azure UDR in the case that FortiGate-A becomes inaccessible. See the diagram below for where this controller node fits. Please contact azure@fortinet.com to obtain this script and get assistance with deployment.


FortiManager
Internet
Azure load balancer
10.40.1.0/24
Public Facing Network
Availability set
Azure FortiGate VM HA Set
SDN Controller Node
VM
10.40.2.0/24
VM
VM
Protected Virtual Network
Microsoft Azure