Section 2

At this point, it is not possible to associate additional NAT rules to the FortiGate within the Azure Preview Portal. Microsoft is aware of the problem and working to resolve it.

The best current workaround is via the Azure CLI

Step 1: Install Azure CLI, following the instructions here:
https://azure.microsoft.com/en-us/documentation/articles/xplat-cli/#how-to-install-the-azure-cli

Step 2: Login to your account:

Note: if you are using a live ID or Microsoft login account, then you will need to create an AD account within your Azure subscription in order to use the Azure CLI. See:
https://azure.microsoft.com/en-us/documentation/articles/resource-group-create-work-id-from-personal/

If you have a work or school account or other AD account associated with your Azure subscription, you can login with the following command:
azure login –u <username> -p

Step 3: configure the Azure CLI to use the new Azure Resource Manager mode:
azure config mode arm

Step 4: Create a new inbound NAT rule on the load balancer:
azure network lb inbound-nat-rule create -g <resource group name> -l <load balancer name> -p <tcp|udp> -f <outside port number> -b <inside port number> -n <rule name>

Step 5: Add the same NAT rule as a target to the outside NIC of the FortiGate VM:
azure network nic inbound-nat-rule add –g <resource group name> -l <load balancer name> -n <network interface name> -r <rule name> --lb-name <load balancer name>

Sample BASH Script:

```
#!/bin/sh

resourceGroup="FortiRG"
loadBalancer="FortiGatepublicLB"
nic="FortiGateNic0"
outsidePort="10443"
insidePort="10443"
ruleName="HTTPS2"

azure network lb inbound-nat-rule create -g $resourceGroup -l $loadBalancer -p tcp -f $outsidePort -b $insidePort -n $ruleName
azure network nic inbound-nat-rule add -g $resourceGroup -n $nic -r $ruleName --lb-name $loadBalancer
```